

3 1761 1155970 0



Task Force on the
Future of the
Canadian Financial
Services Sector


CAI
FN 800
- 1996
F063

Privacy and Financial Services in Canada

by
Richard C. Owens
Smith Lyons

September 1998

Research Paper Prepared for the Task Force on the Future
of the Canadian Financial Services Sector



Digitized by the Internet Archive
in 2022 with funding from
University of Toronto

<https://archive.org/details/31761115559700>



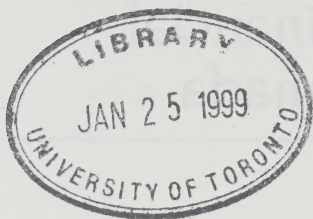
Task Force on the
Future of the
Canadian Financial
Services Sector

Privacy and Financial Services in Canada

by
Richard C. Owens
Smith Lyons

September 1998

Research Paper Prepared for the Task Force on the Future
of the Canadian Financial Services Sector



**The views expressed in these research papers
are those of the authors and do not necessarily reflect
the views of the Task Force on the Future of the
Canadian Financial Services Sector**

Cat No.: BT22-61/3-1998E-11
ISBN 0-662-27150-5

For additional copies of
this document please contact:
Distribution Centre
Department of Finance
300 Laurier Avenue West
Ottawa K1A 0G5

Telephone: (613) 995-2855
Facsimile: (613) 996-0518

Also available through the Internet at
<http://finservtaskforce.fin.gc.ca>

Cette publication est également disponible en français.



Foreword

I am pleased to submit this study to the Task Force on the Future of the Canadian Financial Services Sector.

The Canadian financial services sector is being reinvented at a dizzying pace. Changes are occurring on many levels – competition, structure and ownership, technology. All of these trends have implications for the privacy of customer information.

I am grateful to have had the opportunity to present some views on this important subject, and I hope that they will assist the Task Force in its work.

This study was largely concluded before February 23, 1998 and is current as of that date.

June 1998

Acknowledgements

I take full responsibility for the structure and contents of this study and its conclusions. However, it must be said that its preparation was a group effort and it would not have been possible without substantial contributions, particularly from certain of my colleagues at Smith Lyons. I am especially grateful for the hard work and long hours dedicated by Mr. Thomas Onyshko, an associate with Smith Lyons. Tom's knowledge of the subject greatly contributed to the completion of the study, both through the opportunity to discuss issues with him and by his contributions to its research and writing. Tom was responsible for the initial drafting of major portions of the text and for directing others when I was too busy managing my law practice. Mr. Neil Guthrie, also an associate at Smith Lyons, prepared drafts of substantial portions of this study and assisted with research, and so did Mr. William Schnurr, student-at-law. Other contributions, including research, were made by Mr. Bryce Kraeker, Mr. Simon Crawford and Mr. Ned Djordjevic, students-at-law. Many of them, and particularly Tom, contributed to editing and footnote preparation. The students were especially helpful in proofreading as well. Ms. Tammie Savoie assisted with research and text preparation. The tireless efforts and attentiveness to detail of my assistant, Rosemary Haight, have taken me through this project, like so many others over the past three years. For the professionalism, energy and intelligence of all of them, I thank them. In addition, we profited from the participation and assistance of representatives of financial institutions and consumer advocates. Mr. Thomas Wright, past Privacy Commissioner of Ontario, provided very helpful research suggestions, materials and he brought his experience and insight into the topic to bear by providing us with very useful comments on a draft. I am grateful for the insightful comments of and assistance at various stages in the preparation of this study of Mr. Fred Gorbet, Mr. H. H. MacKay and Mr. John Chant, and other staff members of the Task Force. I am also grateful for the advice of Mr. Tom Smee, a consultant with Deloitte & Touche, on the intricacies of relevant information technology. Finally, I must acknowledge with the deepest gratitude the continued forbearance, moral and intellectual support of my beloved wife, Elizabeth Brubaker.

Table of Contents

Executive Summary	9
I. Introduction	16
Background to this Study	16
Premises of this Study	16
The Nature of Privacy and Informational Privacy Issues	17
The Elements of Privacy	17
The Basis for Privacy Protection	19
Computerization and Personal Information Principles	20
Informational Privacy Issues	22
Privacy Developments Relating to the Financial Services Sector in Canada.....	24
The 1980s: Early Efforts to Implement the OECD Principles	24
The Early 1990s: Reforms to Federal Financial Legislation and Privacy Legislation in Quebec	25
The Late 1990s: The CSA Code, Further Reforms to Federal Financial Legislation and Proposals for Federal Privacy Legislation	28
Public Concern about Privacy and Privacy Complaints.....	33
Public Surveys on Privacy	33
Ekos Research Associates 1992 Survey	33
Louis Harris & Associates/Equifax Canada Inc. 1994 Survey.....	34
FNACQ/PIAC 1994 Survey.....	35
Privacy Complaints About Financial Institutions.....	36
Quebec Commission	36
The Canadian Banking Ombudsman and Internal Bank Ombudsmen.....	38
Insurance Industry Associations	39
Significance of the Data	39
Features of the Financial Services Sector in Canada.....	40
II. Existing Privacy Protection	43
Introduction	43
An Overview of Privacy at Common Law and Equity.....	43
Actions Relating to Intrusion	44
Actions Relating to the Disclosure or Use of Personal Information	45
Contract Law	47
General Shortcomings of Common Law and Equitable Actions	51
The Implied Contractual Duty of Privacy	51
<i>Tournier</i> and the Implied Duty of Confidentiality	51
Implied Terms and Privacy Codes.....	56
Legislative Provisions Respecting Financial Institutions and Confidentiality.....	58

Federal Legislation Relating to Financial Institutions.....	58
Regulation-Making Power Relating to Customer Information	58
Protection and Accuracy of Records	59
Directors' Policies Respecting Confidential Information	60
Restrictions on the Use of Customer Information.....	60
Storing and Processing Customer Information.....	60
Provincial Legislation and Issues	61
Quebec's Private Sector Privacy Legislation	65
Industry Association Codes	68
Canadian Bankers Association	69
Trust Companies Association of Canada	74
Insurance Industry Associations	74
Credit Union Central of Canada.....	77
Observations on Association Codes	77
III. Privacy Challenges	80
Consumer Concerns	80
Sharing and Use of Personal Information	80
Implicit v. Explicit Consent	83
Dispute Resolution Systems and Openness.....	84
Entities Not Regulated by Federal Legislation.....	86
New Technologies and Trends	86
Data Aggregation.....	86
Targeted Marketing and Data Mining	87
Stored Value Cards.....	90
Canadian Internet Banking and Money Management Software.....	91
International Sharing of Information and International Provision of Services.....	92
IV. International Conventions, The EU Directive and Legislation in Foreign and Domestic Jurisdictions.....	94
International Conventions and Agreements Involving Canada.....	94
EU Directive.....	95
The European Approach to Data Protection Legislation.....	95
Development of the EU Directive	96
Council of Europe Convention.....	96
Draft of EU Directive	97
Harmonization of Data Protection Laws throughout the European Union	99
Overview of EU Directive.....	100
"Adequate" Protection and Transfer to Third Countries under the EU Directive.....	102
"Adequate" Protection and Legislation in Third Countries	102
"Adequate" Protection and Contractual Privacy Provisions	104

Privacy Legislation in the United Kingdom	106
Overview of the <i>Data Protection Act, 1984</i>	106
Proposed Changes to the Act in Light of the EU Directive	108
Privacy Legislation for the Private Sector in Quebec	109
Privacy Legislation in New Zealand	110
Overview of New Zealand's <i>Privacy Act 1993</i>	111
Rationale for Extending Privacy Protection to the Private Sector	115
<i>Privacy Act</i> Review	116
Privacy Legislation Developments in Australia	116
V. Privacy, Constitutional Jurisdiction and Federal-Provincial Cooperation	120
Constitutional Jurisdiction Over Privacy	120
Sections 91 and 92 of the <i>Constitution Act</i>	120
Federal Trade and Commerce Power	122
Peace, Order and Good Government	123
Conclusion	125
Models for Federal-Provincial Cooperation	126
VI. Detailed Answers to Questions Posed	131
1. <i>Does existing privacy legislation governing Canadian financial services providers meet the privacy needs of consumers of financial services? If so, are such needs met consistently throughout the financial services industry, or in ways limited to certain types of financial services providers or those of certain jurisdictions?</i>	131
Sufficiency of existing protection	131
Consistency Throughout the Sector	131
Potential Areas of Improvement	132
2. <i>To what extent will new technologies and/or internationalization of the delivery of financial services create a need for additional privacy protection?</i>	133
3. <i>To what extent does privacy regulation need to be tailored specifically to the financial services sector?</i>	134
4. <i>Does the EU Directive, or potentially other legislation requiring reciprocal privacy protection, create a need for additional privacy regulation to facilitate transborder data flows?</i>	135
5. <i>If the need is discovered for additional rules to protect privacy in the financial services sector, on which regulatory structure, given the Canadian context, should it be modeled?</i>	136
Potential Regulatory Models	136
Choosing the Appropriate Model	138
6. <i>What lessons, if any, for Canada can be learned from other efforts to introduce broad privacy protection in a multijurisdictional forum?</i>	139

7. <i>What risks do cross-ownership amongst financial institutions and the provision of multiple financial services by the same entity pose, if any, to privacy?</i>	140
VII. Conclusions	142
Introduction	142
Privacy Interests and the Need for Regulation	142
Privacy Codes	143
Standard Forms and Health Information	145
Credit Bureaux and Insurance Companies	146
Implications of the EU Directive	146
Trends, Technology and Cross-Ownership	146
Appendix A	147
Table of Cases	173
Bibliography	177

Executive Summary

Outline

This study examines concerns arising from the collection and use of personal information by providers of financial services, and considers what additional measures, if any, are required to protect the privacy of consumers of such services. The study is broken into seven main parts.

Part I provides the context for the study as a whole. It considers privacy as both a legal and social concept, and discusses the types of privacy concerns that may arise from the collection and use of personal information. It then reviews various privacy developments relating to the financial services sector that occurred in the 1980s, the early 1990s and the late 1990s. Part I concludes with a discussion of several features of the financial services sector in Canada that must be considered when assessing the need for additional measures to protect privacy.

Part II examines existing forms of privacy protection. The Part begins with a review of the way that common law and equitable actions protect various aspects of privacy, as well as the general shortcomings of such actions. It then discusses the banker's implied contractual duty of privacy, which was recognized in the seminal English case of *Tournier v. National Provincial & Union Bank of England*. Next, the Part considers the way that existing federal and provincial legislation protects privacy. It reviews various provisions in federal laws governing banks, insurance companies, trust companies and credit associations and provincial laws that affect financial services providers including credit bureaux. It also reviews the provisions of Quebec's *Act respecting the protection of personal information in the private sector*, which represents Canada's first data protection statute applying to the private sector as a whole. Part II concludes with a lengthy review of the model privacy codes adopted by the industry associations for banks, trust companies and insurance companies and the model privacy code under consideration by the industry association for credit unions.

Part III discusses potential challenges to the protection of personal privacy. The Part begins by reviewing the key concerns raised by some privacy experts and consumer groups. These consist of the sharing and use of personal information, the use of implicit (as opposed to explicit) consent, the nature of dispute resolution systems, and the fact that various financial services providers are not regulated by federal legislation. The Part then considers technologies and trends with privacy implications: data aggregation, targeted marketing and data mining, stored value cards, Internet banking and money management software, international sharing of information and international provision of financial services.

Part IV discusses international agreements and statutes that protect privacy in certain foreign and domestic jurisdictions. It begins by briefly reviewing international conventions and agreements involving Canada that provide for the protection of privacy. It then turns to a detailed discussion of the European Union's data protection directive; in particular, the discussion considers the restrictions on the international transfer of personal information imposed by the directive. The remainder of the Part discusses the private sector privacy legislation adopted in three jurisdictions and the experience of a fourth jurisdiction that decided against such legislation. The

United Kingdom's *Data Protection Act*, 1994 provides an example of legislation that requires data users to register with a central authority. Quebec's *Act respecting the protection of personal information in the private sector* provides an example of a non-registration system with detailed privacy duties. New Zealand's *Privacy Act* 1993 provides an example of legislation that mixes statutory duties with approved private sector privacy codes. Australia provides an example of a jurisdiction that considered, and then rejected, an extension of data protection legislation to the private sector.

Part V deals with constitutional jurisdiction over privacy in Canada. The Part assesses the merits of competing federal and provincial claims for jurisdiction over privacy matters and concludes that jurisdiction is probably shared by the two levels of government. The Part then discusses some of the conceptual and historical models for federal-provincial co-operation that might inform a shared approach to the regulation of privacy.

Part VI provides detailed answers to the seven questions posed to the authors of this study. Part VI addresses the following issues: the adequacy of existing privacy legislation governing financial institutions; the need for additional protection as a result of new technologies and trends in financial services; the extent to which privacy regulation needs to be tailored specifically to the financial services sector; the degree to which the EU Directive and other foreign instruments create a need for additional privacy regulation, as a result of reciprocal provisions; the appropriate model for additional privacy regulation in Canada, if any; the lessons, if any, that can be learned from other efforts to introduce privacy protection in a multijurisdictional forum; and the risks to privacy that are posed by cross-ownership amongst financial institutions and the provision of multiple services by a single entity.

Part VII sets out the authors' conclusions on the regulation of privacy as it relates to financial services providers. In particular, Part VII discusses privacy interests and the general need for regulation, existing privacy codes used in the financial services sector, standard forms used by financial services providers, the sharing of health information by insurers, the regulation of credit bureaux and insurance companies, the implications of the EU Directive, and the implications of new trends and technologies and the cross-ownership of financial services providers.

Following are brief summaries of the answers to the questions posed to the authors of this study and the general conclusions of this study. Full discussion of the answers and conclusions appears in Parts VI and VII.

Summary of Answers to Questions Posed

- ***Does existing privacy legislation governing Canadian financial services providers meet the privacy needs of consumers of financial services? If so, are such needs met consistently throughout the financial services industry, or in ways limited to certain types of financial services providers or those of certain jurisdictions?***

Existing privacy legislation governing federally regulated financial services providers is not extensive but is substantially augmented by common law and voluntary codes. The consistency of privacy protection varies somewhat throughout the industry, being most highly

developed among larger institutions, particularly the big banks. In general, both the low level of customer complaints about privacy and the extent of existing common law, equity and code-based provisions suggest that existing protection may be adequate. Privacy law outside Quebec is not as consistent as privacy experts might wish, but the costs of imposing additional privacy duties on institutions must be weighed against the benefits likely to be derived. There are various ways that existing privacy codes might be improved to better meet ideal notions of privacy protection. Finally, it is important to note that federal regulation falls only on federal institutions and there are large portions of the financial services sector which are largely unregulated in respect of privacy except in Quebec.

- ***To what extent will new technologies and/or internationalization of the delivery of financial services create a need for additional privacy protection?***

New banking technologies (such as PC- and Internet-based banking) may raise concerns for the security of data communicated over computer networks. However, as financial services providers typically go to great lengths to ensure data security, no additional regulation is needed. It can be expected in the future that “data mining” will be used to a greater extent for targeted marketing purposes by financial institutions. In order to ensure some degree of individual control over personal information, individuals should be permitted to opt out of targeted marketing activities. Internationalization of the financial services sector may raise privacy issues, if it becomes necessary to comply with higher privacy standards in the European Union or if financial institutions operating in Canada seek to use “data havens” for the offshore processing of data. Finally, a concern may arise if a foreign institution offers financial services to Canadians over the Internet without regard to customer privacy; however, the regulatory options available are so limited that the rule of *caveat emptor* likely will continue to apply.

- ***To what extent does privacy regulation need to be tailored specifically to the financial services sector?***

The question might be better put whether privacy regulation *should* be tailored specifically to the financial services sector. In general, the issues concerning collection and handling of personal data are no different for financial institutions than for other businesses. To argue in favour of a tailored approach, one might note that the financial services sector deals with health and financial records – two types of information that raise the highest levels of privacy concerns. On the other hand, because health and financial information is in fact sensitive, legal duties have grown up to protect it which to a large extent obviate the need for further regulation.

- ***Does the EU Directive, or potentially other legislation requiring reciprocal privacy protection, create a need for additional privacy regulation to facilitate transborder data flows?***

Article 25 of the EU Directive states that transfers of data to third countries will be allowed only where there is an “adequate” level of protection in the third country, considered in light of all the circumstances surrounding the proposed transfer. In addition, Article 26 of the EU

Directive permits transfers to third countries without “adequate” protection if one of several exceptions applies. It will be difficult for Canadian policymakers to predict what combination of domestic regulation, legislation and industry codes will meet the requirements of Article 25. As well, the EU Directive owes much to European social and legal traditions and may not sit well within Canada. As a result, Canada may be best served by a policy approach that does not seek to imitate the European model or level of privacy protection. It seems possible that many transfers of personal information between Europe and Canada could continue after implementation of the EU Directive based on contractual privacy protection.

- ***If the need is discovered for additional rules to protect privacy in the financial services sector, on which regulatory structure, given the Canadian context, should it be modeled?***

There are a variety of potential regulatory models available. For example, the United Kingdom provides the example of a system requiring registration before personal information may be processed. Quebec provides the example of a statute which does not require registration but sets out detailed privacy principles which must be followed by the private sector. New Zealand provides the example of a statute that sets out general privacy principles, which may be implemented by approved private sector codes. The model (or the mix of elements from different models) that should be chosen depends on a variety of factors, including the degree of cost, privacy protection and independent review which is desired by the policy maker.

On choosing the correct model for regulation in Canada, it is a reasonable inference that a large scale and rigid regulatory apparatus which imposes substantial expense is more likely to be wrong than a lighter, more flexible form of regulation. The application of a flexible approach is supported by our general conclusion about the need for privacy regulation in the Canadian financial services sector: that, given the low level of privacy complaints and the nature of existing privacy measures relating to the financial services sector, there is no need for change from the status quo. A system which permit rules to be developed and tailored at the industry level is likely to be the most appropriate and effective. In short, Canada’s self-regulatory approach has not failed and may be an appropriate model for the future.

If it is decided to adopt a more stringent legislative approach to privacy protection, an approach based on the New Zealand legislation would be preferable. Privacy principles would be set out in the legislation; these principles could then be enforced through approved industry codes rather than the legislation itself. Such an approach would provide for objective verification of industry codes, thus removing any taint of self-interest. Furthermore, it is our opinion that the present system of oversight would continue to be appropriate in such a system. The Canadian Banking Ombudsman should provide independent review of consumer complaints from the banking industry. Other industries could be encouraged to adopt measures that would provide for independent mediation or arbitration of privacy complaints which could not be resolved internally by institutions.

- *What lessons, if any, for Canada can be learned from other efforts to introduce broad privacy protection in a multijurisdictional forum?*

The experience with the EU Directive suggests that implementing a single directive that will apply to various states may involve a certain degree of compromise. In the Canadian context, it appears that the best results will be achieved if privacy policy is developed jointly with the provincial governments, in part owing to apparent constitutional limitations on the federal power to effect privacy protection. Significant problems may arise in the case of Quebec, since that province has detailed privacy legislation which may not provide a workable model for the federal and other provincial jurisdictions. Ideally, the same general level of protection should exist in all jurisdictions so that national institutions do not have to comply with multiple standards.

- *What risks do cross-ownership amongst financial institutions and the provision of multiple financial services by the same entity pose, if any, to privacy?*

Cross-ownership amongst financial institutions creates the opportunity for sharing of information amongst marketers of different types of financial service to create more accurate marketing. However, the ability to share information amongst service providers or within different divisions of the same service provider has the potential to increase efficiencies and lower costs to consumers. As well, the privacy issues in different parts of the financial services sector do not differ materially. The separation of services into separate legal entities has little to do with any interest of the customer in privacy, but rather with increased ability to regulate, prudential concerns or, most often, the efficacy of industry lobby groups in protecting their economic franchises. Thus, blanket consents on customer contracts which permit the sharing of information within a corporate group are justifiable. Consumer groups have raised the concern that the use of information to try to sell other products could lead customers to feel obliged to buy those products if they are to maintain their banking services. In our view, this case has not been made out.

Summary of Conclusions

- **Privacy Interests and the Need for Regulation:** The existing system of legislation, common law and privacy codes which applies to Canadian financial services providers is one which embodies the principles and aspects appropriate to a modern privacy protection regime. Given the low level of privacy complaints and the sophistication of the best features of the existing system, a cost-benefit analysis would favour a conservative approach to future reforms. If it is determined that a higher level of privacy protection is appropriate, a flexible approach to implementing additional privacy measures should be taken, to allow the regime to best adapt to the industry. Privacy is not at risk only in the financial services sector, although this sector may pose more serious concerns than other sectors of the consumer economy because of the sensitivity relating to health and financial information. There is little difference among federally-regulated, provincially-regulated and largely unregulated financial services providers in their implications for privacy.

- **Privacy Codes:** Modern privacy principles are embodied in model codes adopted by financial industry associations and individual financial institutions. These codes are generally sophisticated and accord a high level of protection to customer privacy. Existing codes might be improved by including provisions which provide further guidance on the use of implied consent, provide greater detail about the purposes for which information may be collected and when information may be collected from third parties, and greater clarity about the reasons for the refusal of access to the individual's information. Privacy codes would preferably permit an individual to opt out of programs which use personal information for targeted marketing. An "opt out" approach is reasonable given that the privacy problem with respect to such practices is not of the greatest magnitude. Privacy codes should be readily available to the public on request. It is a typical provision of a privacy protection regimes that individuals may take unresolved privacy complaints to a regulator or objective referee. In the case of the banking industry, the Canadian Banking Ombudsman plays this role. Other industry associations might be encouraged to establish ombudsmen, or methods of mediation or arbitration to resolve specific disputes. These observations on existing privacy codes do not represent significant shortcomings, but areas for improvement against ideal notions of privacy protection. The codes represent a reasonable basis for self-regulation of the financial services sector.
- **Standard Forms and Health Information:** An area that should be addressed by the industry is the wording of standard forms used by financial services providers. Industry forms that authorize the collection or sharing of information may in some instances be too broadly worded. Health information collected for insurance purposes should not be used to make unrelated decisions (such as credit decisions).
- **Credit Bureaux and Insurance Companies:** Credit bureaux raise significant informational privacy concerns. Existing credit reporting legislation addresses these concerns but it should be reviewed for consistency and comprehensiveness. In addition, the sharing of health information by insurers through the Medical Information Bureau may be a practice which should be governed by appropriate legislation.
- **Implications of the EU Directive:** It would be a mistake to look to the EU Directive on data protection as necessarily providing leadership for Canada concerning privacy protection. Existing measures taken by the financial services sector, particularly if given further legislative sanction through the proposed federal draft regulations, may qualify as "adequate" protection for the purposes of the transfer provisions of Article 25 of the EU Directive. In any case, there is considerable uncertainty over how to comply with Article 25, and a cautious approach is advisable.

- **Trends, Technology and Cross-Ownership:** New technologies and trends generally do not yet raise privacy issues that require a regulatory response. The increased use of “data mining” and direct marketing programs buttresses the conclusion that individuals should be permitted to opt out of such programs by providing notice to their institution. Cross-ownership of financial institutions may cause information to be used by related services providers for a wider range of purposes. Such purposes should be disclosed. However, cross-ownership does not pose a significant enough risk to privacy interests to warrant responses other than as already suggested in terms of the use of health information and opting out of targeted marketing.

I. Introduction

Part I provides the context for the study as a whole. It considers privacy as both a legal and social concept, and discusses the types of privacy concerns that may arise from the collection and use of personal information. It then reviews various privacy developments relating to the financial services sector that occurred in the 1980s, the early 1990s and the late 1990s. Part I concludes with a discussion of several features of the financial services sector in Canada that must be considered when assessing the need for additional measures to protect privacy.

Background to this Study

This study on privacy in the financial services sector was commissioned by the Task Force on the Future of the Canadian Financial Services Sector (the “**Task Force**”) in the Fall of 1997. The terms of reference of the study posed certain specific questions:

1. Does existing privacy legislation governing Canadian financial services providers meet the privacy needs of consumers of financial services? If so, are such needs met consistently throughout the financial services industry, or in ways limited to certain types of financial services providers or those of certain jurisdictions?
2. To what extent will new technologies and/or internationalization of the delivery of financial services create a need for additional privacy protection?
3. To what extent does privacy regulation need to be tailored specifically to the financial services sector?
4. Does the EU Directive, or potentially other legislation requiring reciprocal privacy protection, create a need for additional privacy regulation to facilitate transborder data flows?
5. If the need is discovered for additional rules to protect privacy in the financial services sector, on which regulatory structure, given the Canadian context, should it be modeled?
6. What lessons, if any, for Canada can be learned from other efforts to introduce broad privacy protection in a multijurisdictional forum?
7. What risks do cross-ownership amongst financial institutions and the provision of multiple financial services by the same entity pose, if any, to privacy?

Premises of this Study

This study is based on certain premises. First, this study is concerned with the financial services sector as a whole. This includes federally regulated financial institutions such as banks, trust companies, some insurance companies, and some credit associations, as well as other entities which are subject to varying degrees of provincial or federal regulation, and unregulated financial services providers. The financial services sector has become populated with a wide variety of

institutions. Some are familiar representatives of the four pillars: banks, insurance companies, securities dealers and trust companies. Some are largely unregulated. The unregulated entities that provide services to consumers include business corporations which operate asset-backed lending programs and receivables purchase programs, such as Newcourt Credit, or corporations which operate private label credit card programs, or provide consumer finance. Many such entities are foreign owned.

Second, “privacy” is understood to be a collection of rights of the individual, not corporations. Our discussions with representatives of financial services providers have led us to understand that obligations of confidentiality to corporations are often equated with measures protecting the privacy of personal information. Many of the same systems and precautions serve both ends. However, the protection of the two types of information involves different theoretical justifications. In the case of consumers, the justification is based, in part, on the notion that protection of the individual’s dignity involves an appreciation for personal privacy; in the case of corporations, the justification is based in part on the importance of protecting commercial information that may provide a competitive advantage in the marketplace. In any event, this study relates to consumers and personal privacy only.

Third, privacy is an important human value that should not be sacrificed to the expediency of data users. Based on an appreciation of the value of privacy, this study proceeds to examine the extent to which that value is at risk in the provision of financial services, and precisely how it is at risk. We examine the theoretical basis for privacy protection, and such empirical data concerning threats to privacy in the financial services sector as we could find. We examine the approaches of several foreign jurisdictions, recommendations of other studies and international trends in data regulation. We also review all of the existing law that protects the confidentiality of customer information relating to the provision of financial services. We endeavour to review the matter as thoroughly as possible, within the constraints under which this study was prepared, and to make conclusions based on an objective assessment of the problem.

The Nature of Privacy and Informational Privacy Issues

The Elements of Privacy

In 1890, Boston lawyers Samuel D. Warren and Louis D. Brandeis wrote a seminal law journal article on the right to privacy in tort.¹ Warren and Brandeis provided one of the most popular definitions of the concept of privacy: they defined privacy as “the right to be let alone.” The two lawyers were particularly concerned about invasion of individual privacy by the press, through aggressive reporting of private events and through the use of the new technology of “instantaneous” black and white photography.

Warren and Brandeis’s approach to privacy grew out of the traditional property analysis of the law. At its root, it suggests that society must respect certain property-based boundaries such as

¹ S.D. Warren and L.D. Brandeis, “The Right to Privacy” (1890) 4 *Harvard Law Review* 193. For a critique of the Warren and Brandeis article, see: W.L. Prosser, “Privacy” (1960) 48 *California Law Review* 383.

the sanctity of the home. This approach might have been well suited to the circumstances of the late 1800s, but it is not a product of this modern age, which places increasing emphasis on the importance and economic power of information.

The definition of privacy now widely accepted is one which focuses on control over personal information. In his book *Privacy and Freedom*, Alan F. Westin defined privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”² Westin’s definition has been cited frequently in both academic literature and court decisions.³ It establishes a flexible conception of privacy which depends (at least to some degree) on the preferences of the individual.⁴ While Westin’s definition provides a good starting point, it does not place enough emphasis on the treatment of personal information after its initial communication. Privacy includes also the interest of an individual to be notified of the compilation and exploitation of personal information in ways that alter the individual’s relationship with others. At its core, privacy is about the ability of individuals to negotiate their relationships with others and to establish limits defining the legitimate use of information.

Implicit in much modern thought about privacy is the notion that personal information is the property of the person. However, information does not fit easily into property rights.⁵ While the value of tangible property results from the ability of its owner to physically exclude others from possession, a single piece of information may be fully possessed by many different parties at the same time without affecting it. In addition, there is a legitimate need for the circulation of information about individuals. In fact, personal information *per se* is sometimes as important to a third party as to the individual to whom it relates. For example, my name and address are items of information in which I have some confidentiality interest; but without them, no third party can attribute ownership or other interests to me, or find me when I want them to. My ownership of investments is my information to withhold. I might, for instance, wish to hide my extensive investments (purely hypothetical) in pulp and paper companies from my environmentalist spouse; but that is information I cannot withhold from the institution on whom I rely to maintain detailed and reliable records of those interests. There is a large class of “personal” information which is equally institutional information.

² A.F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 7.

³ See, for example: P. Burns, “The Law and Privacy: The Canadian Experience” (1976) 54 *Canadian Bar Review* at 5 and M. Rankin, “Privacy and Technology: A Canadian Perspective” (1984) 22 *Alberta Law Review* 323 at 325. See also: *R. v. Duarte* (1990), 65 D.L.R. (4th) 240 (S.C.C.) at 252, and *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989) at 763.

⁴ As a report for the Ontario Commission on Freedom of Information and Individual Privacy suggested, privacy “involves establishing a balance between closeness and openness, and the right to privacy is the individual’s right to determine where that balance lies.” See: Ontario, Commission on Freedom of Information and Individual Privacy, *Privacy and Personal Data Protection: Research Publication No. 15* (March 1980) at 13. However, the individual’s ability to control information should have some limits. At times, the individual’s desire for privacy must yield to a larger social need for personal information.

⁵ See generally: R.J. Roberts, “Is Information Property?” (1987) *Intellectual Property Journal* 209 and R.G. Hammond, “Quantum Physics, Econometric Models and Property Rights to Information” (1981) 27 *McGill Law Journal* 47.

There are many aspects to privacy and they should not be confused. "Privacy" means different things in different contexts. For example, in the United States, a constitutional right to privacy has been recognized as the basis for the legalization of abortion.⁶ On the other hand, much privacy thought and study has developed around the compilation of information about individuals by governments, and the risks implied for individual liberties. Privacy is not one thing but many and any analysis must clearly specify which type of "privacy" is under discussion. In our case, this study is focused on informational privacy issues arising in a specific sector (financial services providers) in a particular geographical area (Canada).

The Basis for Privacy Protection

There are a variety of reasons why privacy should be accorded formal protection. Many writers have argued that privacy is necessary for the development of the individual. Privacy provides individuals with physical and intellectual space of their own which encourages individuals to experiment, learn and grow.⁷ Some have argued that privacy is an essential part of intimate relationships such as those between spouses or close friends.⁸ Psychological studies have shown the value of enjoying the time away from the responsibilities and roles imposed by society.⁹ In addition, privacy is important from the point of view of society or the state. Privacy supports a citizenry which is independent and capable of assessing the actions of its government, a requirement for a functional democracy.¹⁰ Privacy may permit individuals to hold and discuss unpopular opinions which, ultimately, will be expressed in public; in this way, privacy may promote a diversity of opinions and the expression of dissenting views.¹¹ In any event, based on survey data, there appears to be a social consensus to the effect that privacy merits protection.

These reasons are not implicated, by and large, in respect of privacy in the financial services sector. The interests with respect to privacy in the financial services sector are principally three. First, an individual has a right to know that his or her sensitive financial affairs and insurance related health and asset information will be kept confidential. The disclosure of such information has the potential to embarrass, to make one the target of envy or of greed, or to adversely affect one's power to negotiate with third parties. For example, the release of transactional information could disclose private political or religious affiliations or sexual proclivities, while the release of health information could expose one to prejudice or lost opportunities for employment, housing or other benefits. Second, an individual has an interest in knowing that the personal information

⁶ For early U.S. Supreme Court decisions recognizing a constitutional right to privacy that protected the ability to make certain types of personal decisions without state interference, see: *Griswold v. Connecticut*, 381 U.S. 479 (1965), *Eisenstadt v. Baird*, 405 U.S. 438 (1972) and *Roe v. Wade*, 410 U.S. 113 (1973). In *Roe v. Wade* the court ruled that the right to privacy provided a basis for a right of access to abortion; this ruling has been narrowed by more recent U.S. Supreme Court decision, although not overturned. For a review of U.S. constitutional privacy law, see for example: Ken Gormley, "One Hundred Years of Privacy" (1992) *Wisconsin Law Review* 1335.

⁷ See, for example: R. Gavison, "Privacy and the limits of law" (1980) 89 *Yale Law Journal* 42.

⁸ See: C. Fried, "Privacy" (1968) 77 *Yale Law Journal* 475 and S.I. Benn, *Privacy, Freedom and Respect for Persons* (Lieber-Atherton, 1971).

⁹ Westin, *supra*, note 2 at 32ff.

¹⁰ See, for example: Gavison, *supra*, note 7, and E.R. Ryan, "Privacy, Orthodoxy and Democracy," (1973) 51 *Canadian Bar Review* 84.

¹¹ Gavison, *supra*, note 7.

collected and used by a financial institution, and on which that institution bases its dealings with that individual, is accurate and up-to-date. Third, an individual may have an interest in not being subject to targeted marketing efforts. While targeted marketing may provide benefit to the individual (in the form of making him or her aware of useful products or services), some individuals may object to this use of their personal information.

An important point to be made in the discussion of the concept of privacy is that privacy cannot be an absolute value. Society involves a balance between the individual and the group; a society of total privacy would not be a society at all but a collection of self-sufficient hermits. Privacy must be balanced against other values in order to achieve social goals. For example, privacy must be compromised if an insurer is to gather details of an insured's claim for payment, a securities dealer is to maintain accurate records of the client's ownership of securities or to comply with the "know your client" rule, or a bank or trust company is to have an address to which to send annuity benefits or account information. There is also a social interest in settling the terms of the collection and use of personal information *en masse* by standard form contracts; this avoids the transaction costs of one on one negotiations to accommodate the privacy preferences of each customer. Finally, if we as consumers demand that financial institutions take a more personal approach and pay greater attention to our individual needs and desires, we must expect that institutions will collect and use our personal information for such purposes.

Another point worth noting is that the concept of privacy is to some extent a cultural value that varies from place to place. For example, writers have argued that significant differences exist between attitudes about privacy and government intrusion in the United States and Europe.¹² Westin, for example, has argued that the U.S. frontier experience has led to stronger resistance to national identification systems, which, in contrast, are common in Europe.¹³ While the concept of privacy varies from society to society, it also varies over time as conditions within a society change. Current notions of privacy in Canada have much to do with patterns of social development over the last century. These patterns include changes to the core definition of the family, a shift in population from small rural communities to large urban centres, an expansion of the sphere of activities of the state and a greater emphasis and the collection of use personal information in both the public and private sector. Individuals living in modern cities likely have a greater degree of anonymity than those living in small towns.

Computerization and Personal Information Principles

Public concern about privacy and the use of personal information spread in the 1960s, when governments and large businesses began to computerize their records. The computerization of personal records meant that personal information could be more easily sorted, combined, transferred and used for new purposes. Ultimately, computerization and the rise of the "information society" led to the growth of new industries that collect, analyze and exploit

¹² See, for example, Herbert J. Spiro, "Privacy in Comparative Perspective" in *Privacy: Nomos XIII*, ed. by J. Rolland Pennock and John W. Chapman (New York: Atherton Press, 1971).

¹³ Alan F. Westin, "Privacy, Technology and Regulation" in *The Computer Culture*, ed. by Denis P. Donnelly (London: Associated University Press, 1985) at 138-139.

personal information.¹⁴ Businesses, including financial institutions, developed new ways to market goods and services to their customers based on the personal information collected through routine transactions. The current capacity to “warehouse” vast quantities of inexpressibly trivial personal information and then “mine” that data for useful nuggets is important to businesses because it may provide them with a competitive advantage in the market.

Initial concern about the spread of computer technology in the 1960s and 1970s lead to the development of principles for the fair treatment of personal information. While these data protection principles address a variety of issues, they deal substantially with privacy concerns. Perhaps the best-known enumeration of personal information principles is set out in the Organization for Economic Cooperation and Development (OECD) guidelines of 1980:

Collection limitation principle: There should be limits to the collection of personal information and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data quality principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose specification principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use limitation principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the purpose specification principle] except with the consent of the data subject or by the authority of law.

Security safeguards principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and the usual residence of the data controller.

Individual participation principle: An individual should have the right:

- (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- (b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him;
- (c) to be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and

¹⁴ For some discussion of the personal information industry, see: Anne Wells Branscomb, *Who Owns Information? From Privacy to Public Access* (New York: BasicBooks, 1994). See also Joseph P. Bigus, *Data Mining with Neural Networks* (New York: McGraw-Hill, 1996).

- (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.¹⁵

The OECD principles represented consensus among OECD members and derive from law reform efforts in several member countries. The principles have played a central role in discussion and debate about informational privacy in Canada. Most recently, they have formed the basis for the Canadian Standards Association's *Model Code for the Protection of Personal Information*.¹⁶

Informational Privacy Issues

Privacy is currently seen to involve a variety of different aspects relating to personal information. First, the privacy interest is implicated in the collection and use of personal information. A key concern of the 1960s and 1970s was the creation of a "womb to tomb" dossier on each individual citizen by government.¹⁷ More recently, privacy experts have pointed to the growth in the collection and use of personal information by the private sector.¹⁸ Businesses now collect information generated by consumer purchases and decisions, and analyse other publicly available information such as census data. Personal information is seen as an asset that may be used to better market products and services to individuals. Privacy experts argue that these developments threaten the individual's ability to control the use of personal information. They contend that individuals should retain some control over the use of their information, so that they may decide, at least to some extent, how, when and for what purposes information is used. At its heart, the issue has much to do with the individual's ability to influence the nature of his or her relationships with government and business institutions.

Second is the disclosure and transfer of personal information. A government or business that has collected information from an individual may transfer or disclose that information so that it becomes available to other parties never authorized or anticipated. For example, a magazine publisher may sell its subscription list to a business wishing to market products or services of potential interest to the magazine's readership. The disclosure and transfer of information raises much the same concern as collection and use. Without controls on the transfer of information, individuals may lose control of their information and their ability to influence their relationships with others. In the case of financial services providers, different divisions of the same institution may use personal information collected from the consumer for one service or product to market other services or products. However, financial institutions are not free to transfer information outside the institution without the consent of the individual. Perhaps the main case of transfer

¹⁵ For the text of the OECD guidelines, see for example James Michael, *Privacy and Human Rights* (Paris: UNESCO Publishing, 1994) at 139ff.

¹⁶ Canadian Standards Association, *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96 (Etobicoke: Canadian Standards Association, 1996).

¹⁷ See, for example: Westin, *supra*, note 2, and Arthur R. Miller, *The Assault on Privacy: Computers, Data Banks and Dossiers* (Ann Arbor: University of Michigan Press, 1971).

¹⁸ See, for example: Willis H. Ware, "The New Faces of Privacy" (1993) 9 *Information Society* 195, and Branscomb, *supra*, note 14.

outside the institution is credit bureau information. Financial services providers provide information about creditworthiness to credit bureaux, which in turn make such information available to other businesses interested in extending credit.¹⁹ Another example of transfer outside the institution relates to the sharing of medical information among insurers. Insurers commonly provide basic medical information on their policy holders to a Massachusetts-based underwriting exchange that makes such information available to other insurers, upon request.²⁰

Third, the inappropriate retention of personal information may threaten an individual's informational privacy. In general, it is desirable that information be deleted once it is no longer relevant to the relationship between the business and the individual. However, information should be retained for certain minimum periods of time to ensure that an individual affected by a decision may gain access to the information on which the decision was based. In addition, it may be appropriate to remove relevant but negative information from the institution's records after long periods of time. The theory here is that personal information should not follow the individual forever: that, after a period of time, the individual should be free from the negative implications of some types of personal information. For example, Ontario legislation governing credit bureaux holds that certain types of information shall not be included in credit reports after certain time limits have passed. Thus, information about an individual's first bankruptcy, non-payment of taxes or fines or convictions of crimes may not be included in credit reports after seven years from the date of the relevant event.²¹

Fourth, personal information must be subject to appropriate security to ensure that it is not subject to unauthorized use or disclosure. Security safeguards may take a variety of forms: policies about who should not have access to information, physical measures to keep certain files or areas secure, dedicated telecommunication lines or networks, and computer hardware or software measures (such as encryption) that prevent access by unauthorized personnel. As well, personal information must be disposed of in ways that ensure that sensitive information does not become available to the public. For example, disposal procedures might require that certain types of sensitive information held on paper be shredded rather merely placed in garbage or recycling bins. While appropriate security and disposal measures are an important part of ensuring informational privacy, they are, for the most part, technical issues. Such issues are not considered in any depth in this study.

Fifth is the interest of the individual to have a right of access to and correction of personal information. To the extent that personal information is used to make decisions affecting the individual, the individual has an interest in the accuracy of such information. The transfer of personal information to other entities in particular makes such access and correction rights more important in order to ensure that the consequences of inaccurate information are not widely ramified. Rights of access and correction have been included in legislation applying to the

¹⁹ For further discussion of credit bureaux, see: Part II, footnotes 201 to 210 and accompanying text.

²⁰ The Medical Information Bureau of Westwood, Massachusetts holds medical information on individual policy holders provided by its member insurance companies in coded form. For further discussion of the Medical Information Bureau, see footnotes 212 to 215 in Part II and accompanying text.

²¹ *Consumer Reporting Act*, R.S.O. 1990, c. C-33, s. 9.

federal and provincial governments in Canada.²² More recently, legislation in Quebec and codes adopted by different industry groups give individuals such rights.²³

Privacy Developments Relating to the Financial Services Sector in Canada

The 1980s: Early Efforts to Implement the OECD Principles

Any analysis of privacy developments relating to the financial services sector in Canada²⁴ must begin with the OECD guidelines, the most influential privacy document to date. Adopted by the OECD in late 1980, the guidelines were intended to form the basis of legislation in the organization's member states, and arose from a concern to protect privacy and the free commercial flow of personal information. At the core of the guidelines is a set of eight principles to be applied to both the public and private sectors: (1) the collection limitation principle, (2) the data quality principle, (3) the purpose specification principle, (4) the use limitation principle, (5) the security safeguards principle, (6) the openness principle, (7) the individual participation principle and (8) the accountability principle. The full text of these principles has been set out earlier in this Part.²⁵

Canada's federal government affirmed its commitment to the OECD guidelines in 1984. Rather than pass legislation applying the OECD principles to the federally regulated private sector, the federal government committed itself to encouraging "private sector corporations to develop and adopt voluntary privacy protection codes."²⁶ In 1985, the federal Department of Justice published a document on the implications of the OECD guidelines.²⁷ In 1987, a Parliamentary committee which reviewed the federal *Privacy Act* recommended that the Act should be extended to the federally regulated private sector.²⁸ However, the federal government's response to the

²² For a general discussion of public sector data protection legislation in Canada, see: Colin H.H. McNairn and Christopher D. Woodbury, *Government Information: Access and Privacy* (Scarborough, Ont.: Carswell, 1992).

²³ The Quebec privacy sector legislation and the codes adopted by industry associations in the financial services sector are discussed at length in Part II of this study.

²⁴ The material discussed under this heading draws heavily on a previous paper: Richard C. Owens, Tom Onyshko, and Peter C. Goode, "Reform Proposals Relating to Customer Privacy and Tied Selling in the Federally-Regulated Financial Services Sector" in *The Regulation of Financial Institutions: Issues and Perspectives* (Scarborough: Carswell, 1997) 143 at 153ff.

²⁵ See the discussion under the Nature of Privacy and Informational Privacy Issues, above in this Part.

²⁶ *Privacy Commissioner of Canada, Annual Report 1984-85* (Ottawa: Supply and Services Canada, 1985) at 11. Commenting on the federal government's move, the commissioner wrote: "This important commitment should be discharged with conviction and vigour and without further delay." However, a year later the commissioner complained in his report that the federal government had done "so little about implementing the OECD guidelines." See: *Privacy Commissioner of Canada, Annual Report 1985-86* (Ottawa: Supply and Services Canada, 1985) at 12.

²⁷ Government of Canada, Department of Justice, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Implications for Canada* (Ottawa: Department of Justice, 1985).

²⁸ *Open and Shut: Enhancing the Right to Know and the Right to Privacy: Report of the Standing Committee on Justice and Solicitor General on the Review of the Access to Information Act and the Privacy Act* (Ottawa: Queen's Printer, 1987) at 77.

review did not express a commitment to extending the Act.²⁹ In the late 1980s, the Minister of External Affairs urged private sector corporations to put the OECD guidelines into practice.³⁰ The Privacy Commissioner's office consulted with the air transportation, banking and telecommunications industries about privacy codes.³¹ Federal officials also met with provincial officials to discuss strategies to encourage the private sector to adopt privacy codes.³²

John Grace was the federal Privacy Commissioner through this period, and his evolving position deserves examination. Immediately after the federal government's 1984 commitment, he signalled his support for an approach promoting voluntary codes in the private sector. He wrote that self-regulation was preferable to government regulation and that privacy protection also was good for business.³³ After the Parliamentary committee review of the *Privacy Act*, he took the position that the government was correct in deciding not to extend the Act to the private sector. He noted that there was no evidence of wide-scale abuse in the private sector, that it was questionable whether the *Privacy Act* could be easily applied to the diverse conditions of different industries and that regulation would require a great increase in the resources committed to the Privacy Commissioner's office.³⁴ However, the commissioner complained about the lack of progress in the adoption of private sector codes.³⁵ Finally, in his 1989-90 report, he called for an amendment to the *Privacy Act* which would require federally regulated corporations to develop privacy codes and submit them to the commissioner's office. Mr. Grace argued that his office could perform a useful monitoring role, although he did not want to play a part in enforcing private sector codes.³⁶

The Early 1990s: Reforms to Federal Financial Legislation and Privacy Legislation in Quebec

The early 1990s saw increasing pressure on federally regulated financial institutions to adopt measures to protect customer information. Reforms to the federal statutes governing financial institutions raised the prospect of regulations on customer information. Bruce Phillips, the federal Privacy Commissioner appointed to replace Mr. Grace in 1991, argued in favour of privacy regulations for financial institutions and of extending privacy legislation to the private sector. The province of Quebec passed privacy legislation applying to the private sector as a

²⁹ See Government of Canada, Department of Justice, *The Steps Ahead* (Ottawa: Department of Justice, 1987).

³⁰ See *Privacy Commissioner of Canada, Annual Report 1987-88* (Ottawa: Supply and Services Canada, 1988) at 8: "The minister of external affairs has called Canada's endorsement to the attention of major Canadian companies and urged that OECD guidelines be put into practice."

³¹ *Privacy Commissioner of Canada, Annual Report, 1989-90* (Ottawa: Supply and Services Canada, 1990) at 13.

³² *Privacy Commissioner of Canada, Annual Report, 1988-89* (Ottawa: Supply and Services Canada, 1989) at 9.

³³ *Privacy Commissioner of Canada, Annual Report 1984-85* (Ottawa: Supply and Services Canada, 1985) at 11.

³⁴ See *Privacy Commissioner of Canada, Annual Report 1986-87* (Ottawa: Supply and Services Canada, 1987) at 6; *Privacy Commissioner of Canada, Annual Report 1987-88* (Ottawa: Supply and Services Canada, 1988) at 7; *Privacy Commissioner of Canada, Annual Report 1988-89* (Ottawa: Supply and Services Canada, 1989) at 9.

³⁵ See, for example: *Privacy Commissioner of Canada, Annual Report 1988-89* (Ottawa: Supply and Services Canada, 1989) at 9.

³⁶ *Privacy Commissioner of Canada, Annual Report 1989-90* (Ottawa: Supply and Services Canada, 1990) at 14.

whole. Industry associations for regulated financial institutions and individual institutions increasingly adopted privacy codes.³⁷

At the beginning of 1990s, the federal government passed wide-ranging reforms to federal legislation governing the financial services sector. These reforms, which came into force in 1992, established the basis of the present financial services environment. As part of the reforms, a new power was inserted into the *Bank Act*, *Insurance Companies Act* and *Trust and Loan Companies Act* giving the federal Cabinet power to make regulations on customer information.³⁸ For example, section 459 of the *Bank Act* gave the Governor in Council the power “to make regulations governing the use by a bank of any information supplied to the bank by its customers.” The government included the regulation-making provisions because of concern about the sharing of information between financial institutions, their affiliates and other parties.³⁹

Also as part of the 1992 reforms, federal regulations governing banks and trust companies prohibited such financial institutions from engaging in the retailing of most insurance products – and from using customer information for that purpose.⁴⁰ Under the regulations, banks and trust companies were prohibited from promoting most types of insurance and prohibited from providing customer information to an insurance company.⁴¹ The ban on the use of customer information for insurance purposes was motivated by a concern that the insurance industry should be protected from competition by banks and trust companies. “Central to the ban on insurance [in the *Bank Act* and regulations] is the issue of target marketing and information flows,” Guy David and Louise Pelly have noted. “The government accepted the insurance industry’s contention that banks would have an unfair advantage if they were permitted to compete with insurance companies.”⁴² The inappropriateness of conflating privacy with measures to promote competitive inefficiency is discussed later in this study.

³⁷ The codes of the Canadian Bankers Association, Trust Companies Association of Canada, Canadian Life and Health Insurance Association, and the Insurance Bureau of Canada are discussed in Part II of this study. It should be noted that CLHIA adopted its privacy guidelines much earlier than the other associations, in 1980. The CBA submitted a model code of privacy principles to its membership in 1986, but this early attempt at a privacy code was rejected by the membership.

³⁸ See the *Bank Act*, S.C. 1991, c. 46, sec. 459; *Trust and Loans Companies Act*, S.C. 1991, c. 45, s. 444; and *Insurance Companies Act*, S.C. 1991, c. 47, s. 489.

³⁹ See: John W. Teolis and Jeffrey S. Graham, *Financial Institutions Reform Package: Phase Two / New Banking Legislation Annotated* (Toronto: CCH Canadian, 1991) at 302. The official explanatory notes on the proposed legislation did not provide much elaboration of the purpose of the sections. For example, in the case of sec. 459 of the *Bank Act*, the official notes state simply: “This section provides for regulations governing the use of confidential customer information. The regulations will be prepared in consultation with the industry and other interested persons.” See: Government of Canada, Department of Finance, *Bank Act Explanatory Notes* (Ottawa: Department of Finance, Winter 1990) at 55.

⁴⁰ See *Bank Act*, S.C. 1991, c. 46, s. 416; *Insurance Business (Banks) Regulations*, SOR/92-330, as amended; *Trust and Loans Companies Act*, S.C. 1991, c. 45, s. 416; and *Insurance Business (Trust and Loan Companies) Regulations*, SOR/92-331, as amended.

⁴¹ See *Insurance Business (Banks) Regulations*, SOR/92-330, ss. 7 and 8; *Insurance Business (Trust and Loan Companies) Regulations*, SOR/92-331, ss. 7 and 8.

⁴² Guy David and Louise S. Pelly Q.C., *The Annotated Bank Act 1996* (Toronto: Carswell, 1995) at 296.

After the 1992 reforms came into effect, the Senate Standing Committee on Banking, Trade and Commerce (the “**Senate Banking Committee**”) held hearings to consider whether the federal government should use the statutory power to make regulations to protect customer information held by financial institutions. Privacy Commissioner Phillips appeared before the committee in support of the idea.⁴³ The Senate Banking Committee commissioned David H. Flaherty (then a professor at the University of Western Ontario with expertise in the area of privacy protection) to develop draft regulations. The July 1992 draft regulations set out a variety of principles similar to those in the OECD guidelines.⁴⁴ In particular, they described principles relating to collection limitation, data quality, purpose specification, use limitation, disclosure of information, security safeguards, individual participation, accountability, openness, liability and external review. The draft regulations are notable for their strict limits on the disclosure of personal information, their requirement that institutions pass corrections to inaccurate personal information to all third parties who have consulted the record, and their commitment to external review of complaints about personal information.⁴⁵ The Senate Banking Committee ultimately concluded in its 1993 report that the federal government should enact regulations. This report stressed the need for independent review of privacy complaints and recommended the creation of a new financial sector privacy protection agency to fulfil this function.⁴⁶

In January 1994, Quebec’s *Act respecting the protection of personal information in the private sector* (also known as Bill 68) came into force.⁴⁷ The Act applies to a wide range of private sector entities, including corporations, sole proprietorships, partnerships, organizations and associations.⁴⁸ Various provisions govern the collection, use and transfer of personal information; the Act also establishes the individual’s right to gain access to personal information and request a correction where it appears inaccurate. Special provisions apply to lists of names used for marketing purposes and also to transfers of information about Quebec residents to third

⁴³ Standing Senate Committee on Banking, Trade and Commerce, *Interim Report on the 1992 Financial Institutions Legislation* (August 1995) at 9.

⁴⁴ *Regulations on the Use by Financial Institution of any Information Supplied to the Financial Institution by its Customers, Prepared for the Standing Senate Committee on Banking, Trade and Commerce* (Ottawa: Library of Parliament Research Branch, 30 July 1992).

⁴⁵ On the question of disclosure, Flaherty’s proposals included the following: in general, there should be no disclosure of personal information without the express, written consent of the customer; banks should notify customers of legal orders requiring the disclosure of information; all third party requests for customer information should be in writing and specify the reason for the request; financial institutions should not be permitted to use personal information for direct marketing purposes without the express, written consent of the customer; in general, financial institutions should not be permitted to disclose personal information to subsidiaries or affiliated companies; and personal information disclosed to third parties for the purpose of providing goods or services (e.g., printing customer cheques) should be protected by contractual terms requiring adherence to the regulations. On the question of review, Flaherty proposed that the Office of the Superintendent of Financial Institutions would be required to investigate privacy complaints and would have the power to order banks to address such complaints.

⁴⁶ *Regulations on the Use by Financial Institution of any Information Supplied to the Financial Institution by its Customers: Final Report of the Standing Senate Committee on Banking, Trade and Commerce* (Ottawa: Queen’s Printer, June 1993) at 1 and 3.

⁴⁷ The Act fleshes out provisions included in the new *Civil Code of Quebec*, passed in 1991: S.Q. 1991, c. 64, articles 35-41.

⁴⁸ See: R.S.Q. c. P-39.1, s. 1 and *Civil Code of Quebec*, article 1525.

parties outside the province.⁴⁹ Disputes under the Act are to be resolved by the body responsible for resolving disputes under Quebec's public sector access and privacy statute, the Commission d'accès à l'information. While there is some question about whether the Act's application to banks is constitutional, at least one commentator has suggested that it would survive a constitutional attack.⁵⁰ The Act raised important implications for the country as a whole, since Canada became "the only country in which the scope of privacy protection in one of its member jurisdictions exceeds that of the federal government."⁵¹

In the mid-1990s, Privacy Commissioner Phillips called for the federal *Privacy Act* to be extended to the federally regulated private sector. In his 1995 annual report, he wrote that he no longer supported an approach based on voluntary codes. His reasons included the growth of the personal information industry, the rapid pace of technological change and the threat to public sector privacy protection posed by the increasing "interconnectivity between public and private sector data bases and transmission systems."⁵² The commissioner proposed new legislation that would apply to both the public and private sectors and would create an independent oversight mechanism.

The Late 1990s: The CSA Code, Further Reforms to Federal Financial Legislation and Proposals for Federal Privacy Legislation

The late 1990s have seen further developments in the area of privacy. These developments include the Canadian Standards Association's model privacy code, reforms to federal financial legislation that include a broader power to regulate on customer information matters, and recent federal proposals for privacy legislation applying to the private sector.

In 1996, the Canadian Standards Association (CSA) adopted its *Model Code for the Protection of Personal Information*.⁵³ The CSA model code was drafted by a committee of representatives of business, government and consumer groups. It sets out 10 principles on privacy and the individual's right of access to information that borrow heavily from the OECD guidelines:

Accountability: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

⁴⁹. See: R.S.Q. c. P-39.1, s. 17 and ss. 22-26.

⁵⁰. See: Etienne Dubreuil, "Quebec Bill 68: Is It Sufficient for the Federal Canadian Financial Institutions Sector?" in *Privacy in Financial Services* (Toronto: Canadian Institute, 1994).

⁵¹ Colin J. Bennett, *Implementing Privacy Codes of Practice* (Toronto: Canadian Standards Association, 1995) at 10.

⁵². *Privacy Commissioner of Canada, Annual Report 1994-95* (Ottawa: Canada Communications Group, 1995) at 4.

⁵³ The CSA is a non-profit organization that develops standards in areas such as health, safety and environmental protection.

Consent: The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Limiting Use, Disclosure and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

Accuracy: Personal information shall be as accurate, complete and up-to-date as necessary for the purposes for which it is used.

Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of information.

Individual Access: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.⁵⁴

The CSA model code is intended to serve as a model which may be voluntarily adopted by a business, after modifications are made to better reflect the particular industry of the business. It has been recognized as a workable model by the federal Privacy Commissioner and government officials.⁵⁵ After the publication of the model code, the industry associations representing banks and property and casualty insurers revised their model privacy codes to comply with the new CSA standard.

Also in 1996, the federal Department of Finance issued its White Paper on proposed 1997 reforms to the federal legislation governing financial institutions. The White Paper discussed possible reforms relating to several consumer protection issues including privacy. The paper stated that the protection of privacy was of utmost importance because new technologies permitted the easy collection and analysis of personal information.⁵⁶ While acknowledging the efforts of the financial services industry to address privacy issues, the paper argued that further steps were required. It proposed a government regulation that would require financial institutions to adopt codes of conduct governing the collection, use, retention and disclosure of

⁵⁴ Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada*, CAN/CSA-Q830-96 (Etobicoke, Ont.: CSA, 1996) at ix.

⁵⁵ See, for example, *Privacy Commissioner of Canada, Annual Report 1994-95* (Ottawa: Canada Communications Group, 1995) at 14-15.

⁵⁶ Government of Canada, Department of Finance, *1997 Review of Financial Sector Legislation: Proposals for Changes* (Ottawa: Department of Finance, June 1996) at 15.

information. In addition, the proposed regulation would require financial institutions to designate senior officials to implement privacy complaints procedures and require financial institutions to report annually on privacy complaints received and the steps taken to address such complaints. Observers later argued that the privacy proposals were unnecessary – and harmful to the reputation of the industry – given the lack of any evidence of a privacy problem in the financial services sector.⁵⁷

Both the House of Commons Standing Committee on Finance (“**House Finance Committee**”) and the Senate Banking Committee released reports that included comments on the privacy issues raised in the White Paper. The House Finance Committee report recommended that government regulations should require financial institutions to provide customers with written information on their privacy code and details of how customers could make complaints.⁵⁸ As well, the report recommended that a new federal body – the Consumer Protection Bureau – be established to hear privacy complaints. Finally, the report recommended that “the issue of market power that financial institutions derive from the massive amount of data and information available to them is one that should be considered by the Task Force.”⁵⁹ The Senate Banking Committee supported the government recommendations set out in the White Paper.⁶⁰

A further development in 1996 deserves consideration. The federal ministers of Industry and Justice made a commitment to developing new legislation to protect the privacy of personal information in the private sector. Industry Canada’s report *Building the Information Society* noted that in order to address public concerns about the misuse of personal information, new legislation must recognize the individual’s right to privacy in the electronic world. “The right to privacy must be recognized in law, especially in an electronic world of private databases where it is all too easy to collect and exploit information about individual citizens.”⁶¹ The report stated that the federal ministers of Industry and Justice would consult with the provinces to develop proposals for a “legislative framework” for the protection of personal data in the private sector. Later, the Minister of Justice promised that the new privacy legislation would be passed by the year 2000.⁶²

In 1997, Parliament passed legislation embodying the proposed privacy reforms set out in the Department of Finance’s 1996 White Paper. Among other amendments, Bill C-82 added an expanded regulation-making power to the *Bank Act*, the *Trust and Loan Companies Act* and the *Insurance Companies Act*.⁶³ The new power permitted the government to issue regulations

⁵⁷ See: Owens, Onyshko and Goode, *supra*, note 24.

⁵⁸ *Fourth Report of the House of Commons Standing Committee on Finance, 1997 Review of Financial Sector Legislation: Proposals for Change* (October, 1996) at 3-4.

⁵⁹ *Ibid.*, at 4.

⁶⁰ *Standing Senate Committee on Banking, Trade and Commerce, 1997 Financial Institution Reform: Lowering the Barriers to Foreign Banks* (October 1996) at 32.

⁶¹ Government of Canada, Department of Industry, *Building the Information Society: Moving Canada into the 21st Century* (Ottawa: Department of Industry, 1996) at 25.

⁶² Notes for An Address by The Honourable Allan Rock, Minister of Justice and Attorney General of Canada, to the Eighteenth International Conference on Privacy and Data Protection (Ottawa, September 18, 1996).

⁶³ S.C. 1991, c. 46, s. 459 as amended by 1997, c. 15, s. 55; S.C. 1991, c. 45, s. 444 as amended by 1997, c. 15, s. 385; S.C. 1991, c. 47, s. 489 as amended by 1997, c. 15, s. 263.

requiring a financial institution to establish procedures on the collection, retention, use and disclosure of any information about its customers. The new power also permitted regulations that required institutions to implement privacy complaint procedures and to make reports to regulators on the complaints received. It is expected that the government will issue new regulations under this power as early as the Summer of 1998.

In late 1997, the Ontario Ministry of Health released a proposed *Personal Health Information Act*.⁶⁴ The proposed Act would regulate the use of health information by various parties including the provincial Ministry of Health, hospitals and insurance companies licensed under the Ontario *Insurance Act*.⁶⁵ Such parties would be required to follow privacy principles relating to the collection, use and disclosure of health information; as well, they would be required to provide rights of access to an individual's own health information. The insurance industry has expressed concern that if Ontario and other provinces enacted health information statutes, it could become subject to statutory privacy duties that varied from province to province.⁶⁶ (The governments of Manitoba and Alberta have introduced medical information Bills, although the provisions of these Bills would not appear to apply to insurers.⁶⁷) However, insurance companies have in the past shared information through central agencies such as the Medical Information Bureau of Massachusetts. Just as credit bureaux are regulated because of the risk entailed to a consumer if information held about her is inaccurate, it would be appropriate to regulate the information sharing activities of insurers.

In January 1998, the federal Departments of Industry and Justice issued a discussion paper about proposed federal privacy legislation for the private sector.⁶⁸ The discussion paper proposes a new federal law that would apply across the federally regulated private sector, coupled with new provincial legislation that would apply to the provincially regulated private sector. The implication is that the federally regulated financial services sector would fall within the scope of

⁶⁴ Government of Ontario, Ministry of Health, *Personal Health Information Protection Act, 1997: Draft for Consultation* (November 1997), available at <http://www.gov.on.ca/health>. See also: Government of Ontario, Ministry of Health, *Draft Personal Health Information Protection Act, 1997: Overview* (November 1997).

⁶⁵ For a list of parties covered, see the definition of "health information custodian" in s. 2 of the draft Act.

⁶⁶ Canadian Life and Health Insurance Association, Inc., *Privacy and Financial Institutions: Input to Mr. Owens and Mr. Wright re Task Force Research Project* (December 1997) at 6: "There is some concern...about possible inconsistencies arising as further regulation is developed at the provincial level."

⁶⁷ See: Manitoba's *Personal Health Information Act, 1997* (Bill 51) and Alberta's *Health Information Protection Act, 1997* (Bill 30). In the case of the Manitoba Bill, the definition of a "trustee" of health information provided in s. 1 suggests that the Bill would not apply to a private sector entity such as an insurance company. In the case of Alberta Bill, a review of the provisions of the Bill suggests it is aimed at the public and health care entities. However, the definition of a "custodian" of health information in s. 1 includes "any...corporation or other body that is designated in the regulations as a custodian." Thus, insurance companies and others could be added by regulations. A background paper about the Alberta Bill does not mention plans to add insurance companies: see <http://www.health.gov.ab.ca/whatsnew/releases/protect.htm>.

⁶⁸ Government of Canada, Departments of Industry and Justice, *The Protection of Personal Information: Building Canada's Information Economy and Society* (Ottawa: Department of Industry, January 1998), available at <http://strategis.ic.gc.ca/privacy>. See also Jeff Sallot, "Ottawa Weaving Tight Web Privacy Law," *Globe & Mail*, 27 January 1998, at A1 and A12.

the new federal privacy law.⁶⁹ The discussion paper raises a series of questions about the shape of new legislation and seeks public input on these questions.

The federal discussion paper suggests that the 10 principles from the CSA model code should form the basis for new legislation. However, it questions whether the language of the principles is specific enough for legislation, and whether additional duties not included in the principles should be considered. The paper raises the issue of the role that privacy codes might play in the new legislative environment. It notes that approved codes might serve as an aid to interpreting the legislation or even replace the privacy duties set out in legislation, as in the case of the legislation of the Netherlands and New Zealand, respectively. On the other hand, it notes that the new law might simply ignore codes or fail to give them any legal effect. Finally, the paper discusses various enforcement issues. Here, it suggests a process that would see privacy complaints taken first to the institution and then, if the individual remains unsatisfied, to a government review body. It leaves open the question of the identity of the review body, suggesting that it might be either the regulator responsible for the particular institution or a general privacy official, such as the federal Privacy Commissioner.

The discussion paper notes that a national law reform organization known as the Uniform Law Conference of Canada (ULCC) is in the process of drafting a model privacy law which might serve as a template for new federal and provincial legislation. The ULCC's efforts date back to 1995, when it began discussions on the need for a model law governing the use of personal information in the private sector.⁷⁰ In March 1998, lawyers charged with developing the model law for the ULCC produced a second draft based on the CSA principles.⁷¹ The second draft imposes general duties on private sector organizations, and suggests that detailed procedures for obtaining consent from individuals and charging individuals fees for access would be set out in supporting regulations. The second draft gives a privacy commissioner the power to investigate complaints and make recommendations to the parties. If a complaint was not resolved by this process, the individual could refer the matter to a privacy tribunal. The tribunal would have the power to make binding orders, including an order compensating the individual for harm caused by a contravention of the Act. It is expected that the second draft will be further modified; ultimately, the proposed draft will be set before the ULCC's annual meeting in August 1998, when it may be adopted by the organization's membership. Assuming that the Model Act is adopted by the ULCC, it may serve as a model for federal and provincial law reform.

⁶⁹ *The Protection of Personal Information*, *supra*, note 68 at 16. The paper mentions the Canadian Bankers Association 1996 model code as an example of efforts at self-regulation, without making any suggestion that the new federal law would not apply to banks.

⁷⁰ For the first ULCC report on the concept of a model law, see: Denis C. Kratchanov, *The Uniform Law Conference of Canada: Personal Information and the Protection of Privacy* (1995), available at <http://www.law.ualberta.ca/alri/ulc/95pro/e95m.htm>.

⁷¹ Fax from Denis C. Kratchanov, Department of Justice (Canada) to T.S. Onyshko, dated March 5, 1998, with text of draft *Private Sector Protection of Personal Information Act* attached.. The first version of the second draft, which dealt with most of the model law's provisions except for those relating to enforcement issues, was released in the Fall of 1997: see Fax from Denis C. Kratchanov to T.S. Onyshko, dated December 15, 1997.

Public Concern about Privacy and Privacy Complaints

Public Surveys on Privacy

Recent surveys have shown high levels of concern about privacy, although the extent to which individuals have actually experienced invasion of privacy remains unclear. These surveys also reveal conflicting evidence as to whether Canadians are confident in the ability of business to self-regulate in the area of privacy protection. Three Canadian surveys deserve particular discussion: the 1992 Ekos Research Associates survey for various parties, the 1995 Louis Harris & Associates survey for Equifax Canada Inc. and the 1994 survey by consumer groups FNACQ and PIAC.

Ekos Research Associates 1992 Survey

In 1992, Ekos Research Associates Inc. conducted a survey of 3,000 Canadian households on behalf of a variety of public and private sector parties.⁷² The survey found that concern about privacy was “remarkably high”: 92 per cent of respondents expressed moderate or greater concern about privacy.⁷³ There was evidence of particular concern about personal information. Respondents were asked to indicate how important five different aspects of privacy were to them; later, the results were ranked based on the number of people who expressed extreme concern about particular aspects. The ranking placed informational privacy aspects in the second and third position (i.e., “controlling who gets information” and “controlling what information is collected”) before aspects relating to privacy at home and at the workplace (i.e., “not being disturbed at home” and “not being monitored at work”).⁷⁴

The Ekos survey also revealed particular concern about financial and health information. Respondents were asked to rate their level of concern for requests for 10 types of information; the results were later ranked based on the number of people who expressed extreme concern about a particular type of information. This ranking showed that the highest levels of concern existed for information relating to the individual’s financial situation, health records and buying habits.⁷⁵ However, it is worth noting that the degree of concern in providing personal information varied depending on the source. Responses about the degree of concern involved in providing personal information to 13 types of organizations were ranked, with insurance companies ranking seventh and banks ranking eighth.⁷⁶ Organizations ranked as involving higher levels of concern were companies that sell to people at home, survey companies, telephone companies, retail stores, credit bureaux and television cable companies.

⁷² Ekos Research Associates Inc., *Privacy Revealed: The Canadian Privacy Survey* (Ottawa: Ekos Research Associates, 1993).

⁷³ *Ibid.*, at i.

⁷⁴ *Ibid.*, at 10.

⁷⁵ *Ibid.*, at 20.

⁷⁶ *Ibid.*

When respondents to the Ekos survey were asked to discuss their own experience, 18 per cent claimed to have experienced a “serious” invasion of privacy.⁷⁷ These experiences fell into eight broad categories, consisting of: physical threats or criminal incidents; nuisances or disturbances; verbal or psychological harassment; abuse of information, government intrusion or release of information without consent; incidents involving credit or financial matters; incidents involving the police; spying or trespass; and incidents involving the workplace. At least some of these experiences appear to involve issues far from the central concerns of privacy experts. And, as the study itself noted, a large majority of Canadians had not experienced a serious invasion of privacy: “This suggests that many people’s concerns are based on other factors. These factors may include: matters of principle, hypothetical situations, concern about these problems applying to them or their families in the future, or the experiences of friends and family.”⁷⁸

Finally, the Ekos survey found that there was a public desire for action to address privacy concerns and that “[t]he strongest support is for an active involvement of government – either on its own or in partnership with business.”⁷⁹ A majority of respondents agreed with statements that government should pass legislation to ensure that privacy is protected, privacy rules should apply to both government and business, and government should work with business to develop guidelines to protect privacy. In contrast, a minority of respondents agreed that they were confident privacy would not be threatened if business was responsible for regulating itself.

Louis Harris & Associates/Equifax Canada Inc. 1994 Survey

In August and September 1994, Louis Harris & Associates conducted a survey of 1,250 Canadians for Equifax Canada Inc., a major credit reporting company.⁸⁰ The survey found that high levels of concern about privacy existed: 70 per cent of respondents agreed with the statement that “Consumers have lost all control over how personal information about them is circulated and used by companies.”⁸¹ However, in accord with the 1992 Ekos survey, the Harris survey found that a minority of respondents (22 per cent) had actually experienced an “improper” invasion of privacy.

The survey provided evidence of public support for certain uses of personal information. There was strong support for the collection and use of personal information to assess credit risks. Large majorities of respondents accepted that credit bureaux should collect and provide personal information for an informed assessment of the risk on bank loans, home mortgages and credit cards.⁸² The survey also suggested that consumer concern relating to the use of personal information focused more on the transfer of information outside the institution than the use of

⁷⁷ *Ibid.*, at 15.

⁷⁸ *Ibid.*

⁷⁹ *Ibid.*, at 28.

⁸⁰ The 1994 Louis Harris & Associates survey was a follow up to a 1992 survey for Equifax Canada Inc. by the same polling organization.

⁸¹ *The Equifax Canada Report on Consumers and Privacy in the Information Age* (Equifax Canada Inc., 1995) at 17.

⁸² *Ibid.*, at 43

information by the institution for a new purpose.⁸³ For example, 79 per cent of respondents would find it acceptable for a bank to send unsolicited information on mortgage rates to its customers. However, 69 per cent of respondents would find it unacceptable for a financial company with which they do business to provide their name and address to an affiliated investment company, so that the investment company could mail them an offer for a market investment account.

A number of further findings supported industry self-regulation as an answer to privacy concerns. A majority of 74 per cent of respondents agreed with the statement: "If companies and industry associations adopt good voluntary privacy policies, that would be better than enacting government regulation."⁸⁴ More respondents were concerned about invasion of privacy by the government than about invasion of privacy by the private sector.⁸⁵ And a majority of respondents indicated that when choosing a bank or health insurer it would be "very important" whether the institution had adopted a strong privacy protection policy.⁸⁶

FNACQ/PIAC 1994 Survey

Two public interest groups, Montreal's Fédération nationale des associations de consommateurs du Québec and Ottawa's Public Interest Advocacy Centre, conducted a survey of 2,000 Canadians in December 1994.⁸⁷ The study suggested that, despite the findings of earlier research, individuals had substantial personal experience of privacy intrusions:

Earlier research had argued that for many Canadians it was vicarious or theoretical possibility of insidious, hidden invasions which produced highest levels of concern. This new study clearly documents that many informational privacy abuses are in fact fairly pervasive, and indeed noticed by individuals. On the other hand it is quite clear that the level of experience is inversely correlated with the seriousness of the invasion. In other words, relatively trivial invasions (e.g., "victims" of telemarketing) are ubiquitous, but more threatening forms of privacy invasions, such as governments selling your health history to an insurance company or an employer taping your telephone conversations, are relatively rare.⁸⁸

The FNACQ/PIAC survey identified several activities with privacy implications which more than 50 per cent of respondents had experienced or believed they had experienced: uninvited calls from businesses, being required to provide information about employment status when

⁸³ *Ibid.*, at xiii and 20-22.

⁸⁴ *Ibid.*, at 17.

⁸⁵ *Ibid.*, at 18: "When asked which type of invasions of privacy worry them most, 51% of Canadians indicate that they are most concerned about the activities of government agencies, compared with 37% who are more worried about the activities of business."

⁸⁶ *The Equifax Canada Report on Consumers and Privacy in the Information Age* (Equifax Canada Inc., 1995) at 19-20.

⁸⁷ Public Interest Advocacy Centre and Fédération nationale des associations de consommateurs du Québec. *Surveying Boundaries: Canadians and their Personal Information* (Ottawa and Montreal: PIAC and FNACQ, 1995).

⁸⁸ *Ibid.*, at x-xi.

opening a bank account, uninvited calls from charities, businesses monitoring personal information in order to target market goods and services, and calls from organizations when the individual had called but not left a message for a return call.⁸⁹ Other activities which a significant number of respondents had experienced or believed they had experienced included businesses selling personal information, businesses sharing personal information with affiliates, and charities selling lists of names.⁹⁰ However, many of these activities – including the most common (i.e., uninvited business and charity calls) – were viewed as “very serious” by only a minority of respondents.

On the issue of the manner of privacy protection, the FNACQ/PIAC survey suggested that the public had a strong preference for government involvement, although there was distrust of both government and the private sector. Eighty-seven per cent of respondents agreed that the protection of personal information should be a “priority” of government, although a large majority also rejected the notion that they should have to pay higher taxes for better privacy protection.⁹¹ The survey authors argued that the results of 1994 Harris/Equifax survey supporting self-regulation could be explained by the fact that the question used there was qualified (i.e., “If companies and industry associations adopt *good* voluntary policies....”).

Privacy Complaints About Financial Institutions

While the surveys discussed above reveal high levels of concern about privacy, there is little or no evidence that consumers are experiencing serious privacy problems in their dealings with financial institutions. There are three main sources of statistics and information about privacy complaints involving financial institutions: the Quebec access and privacy commission, the Canadian Banking Ombudsman and individual bank ombudsman, and the insurance industry associations. All report low levels of complaints about privacy issues.

Quebec Commission

The Commission d'accès à l'information du Québec is the provincial agency with a mandate to receive, investigate and resolve complaints under Quebec's private sector privacy law. In 1995-96, the commission received 151 complaints relating to the private sector as a whole, of which 13 per cent (or 20 complaints) related to financial institutions and 14 per cent (or 21 complaints) related to insurance companies.⁹² Information about the nature of complaints to the Quebec commission suggests that they deal with cases in two main categories: those

⁸⁹ *Ibid.*, at 6.

⁹⁰ *Ibid.*, at 6. Twenty-five to 39 per cent of respondents indicated that they had experienced, or believed they had experienced, these activities.

⁹¹ Public Interest Advocacy Centre and Federation nationale des associations de consommateurs du Québec. *Surveying Boundaries: Canadians and their Personal Information* (Ottawa and Montreal: PIAC and FNACQ, 1995) at 36-37.

⁹² Commission d'accès à l'information du Québec, *Vie privée et transparence administrative au tournant du siècle* (Juin 1997) at 1.3.3 and Graphique 10, available at <http://www.cai.gouv.qc.ca/sunset1.htmk>. The paper does not discuss the commission's definition of a “financial institution,” which apparently does not include an insurance company.

involving the collection or disclosure of information without consent, and those involving the wording of forms obtaining individual consent.⁹³

As an example of a complaint in the first category, one bank was alleged to have gathered information about a woman who applied for a car loan, including information about her alimony payments and rent, and then provided this information to her employer. The commission found that the complaint was justified as the form did not provide proper consent to the disclosure, and ordered the bank to take corrective measures. In another case, a trust company revealed that the complainant had three G.I.C.s in particular amounts to the complainant's wife. The trust company was closing the particular branch and wanted to provide notice to the complainant. Although there was no bad faith on the part of the trust company, there was a violation of the Quebec Act when the trust company disclosed information to a third party. And in a case involving a *caisse populaire*, the commission found that the institution had disclosed the complainant's bankbook to a lawyer after the lawyer issued a subpoena referring to the information. The commission noted that the lawyer did not have the power to compel disclosure, and that the institution should have appeared before the tribunal with the information. Other example cases involved situations where financial institutions ran credit checks without proper consent or revealed confidential information to the ex-wife of the complainant or another party.⁹⁴

As an example of a complaint in the second category, a consumer group filed a complaint against an insurance company based on the wording of the consent form which an insured would sign to claim payment of medical expenses. The form authorized every doctor, hospital, clinic or government institution to provide the insurer with any information requested on the medical history of the patient. The commission found that there was no need for the insurer to have access to all the claimant's medical records in order to process a particular claim. The insurer was ordered to revise the form. In another case of this type, the complainant wished to make a claim on his insurance policy and was required to sign a form allowing the insurance company to gather and communicate any personal information concerning the complainant. The commission ruled that the claim form was too broad to provide proper consent, and the insurer was ordered to redraft the form. And in another case, the complainant challenged a bank policy that required a new customer to produce three pieces of identification in the form of a social insurance number, a health card and a credit card. The commission ruled that the complaint was partially justified:

⁹³ The following discussion of complaints to the Quebec commission is based on materials about complaint investigations and decisions provided by the Commission d'accès à l'information du Québec to the authors of the study in December 1997. See: Letter to B. Schnurr from Christiane Cliche of the Commission d'accès à l'information du Québec of December 9, 1997. A representative of the commission indicated that the material could be published in this study.

⁹⁴ For example, a complainant alleged that a bank had revealed confidential information to his ex-wife (i.e., his bank account balance) which caused him serious problems. The commission found that there was a violation of the Quebec Act and that the bank must take measures to ensure a similar situation would not occur in the future. In another case, the complainant had received confidential information from a bank about another party, presumably by mistake. After being informed of the incident, the bank took appropriate measures to ensure the situation would not occur again. And in other cases, a *caisse populaire* and an insurance company failed to obtain proper consent before running credit cheques on individuals. The insurance company alleged that the individual had given oral consent, which the individual disputed. However, the commission noted that in cases of doubt the onus was on the institution to show that proper consent had been obtained.

although the bank could ask for identification, it could not demand that specific pieces of identification be produced.

The Canadian Banking Ombudsman and Internal Bank Ombudsmen

The office of the Canadian Banking Ombudsman (the “**Ombudsman**”) was established by the banking industry in 1996. The Ombudsman’s office is funded by major banks operating in Canada, and responsible to a board of directors consisting of five bankers and five independent directors.⁹⁵ Originally, the Ombudsman’s mandate was the resolution of complaints from small businesses; however, the mandate was expanded to include the resolution of complaints from individuals, which have been accepted since March 1997. The Ombudsman may investigate a consumer complaint against a participating bank if the consumer has used the bank’s internal complaint procedure and remains unsatisfied. After an investigation, the Ombudsman may issue a non-binding recommendation to the bank. Statistics about the level and nature of consumer complaints to the Ombudsman’s office were released in July 1997.⁹⁶ They show that in the first five months of accepting consumer complaints, the Ombudsman received 198 such complaints. Of these only two complaints – or 1 per cent of the total – related to privacy issues.

One of these privacy complaints to the Canadian Banking Ombudsman involved the following situation.⁹⁷ Mr. X had applied to establish a line of credit at a branch where he and his wife, Ms. X, had a joint mortgage and joint bank account. Ms. X did not provide consent to the bank to obtain a credit report on her; however, the bank later showed a credit report about Ms. X to Mr. X. Ms. X. later complained that her privacy had been violated. The bank defended its actions saying that since other bank transactions had been joint, it presumed the application for a line of credit was joint as well. The Canadian Banking Ombudsman investigated the incident and determined that the bank had breached its own policies and several of the privacy principles in the Canadian Bankers Association model code. The breaches included showing a credit report to a third party outside the bank and relying on a 10-year old consent to obtain a credit report. The complaint was resolved when the bank paid Ms. X. \$4,000 for expenses and lost wages relating to her year-long effort to get the bank to acknowledge her privacy had been violated.

The other privacy complaint involved a telephone application for an RRSP loan.⁹⁸ The bank representative asked the customer the name of his employer but did not obtain permission to contact the employer. The bank later contacted the customer’s employer, and defended itself by claiming that the customer should have known that verification of employment was part of the lending process. The Canadian Banking Ombudsman concluded that the bank violated its own

⁹⁵ Canadian Banking Ombudsman, *1996 Annual Report*; and Canadian Banking Ombudsman, *Submission to the Task Force on the Future of the Canadian Financial Services Sector* (North York: October 1997).

⁹⁶ Canadian Banking Ombudsman, *Report for the Nine Months ended July 31, 1997* (1997).

⁹⁷ Canadian Banking Ombudsman, “Privacy Case Summary” (November 17, 1997), a short document provided by the Ombudsman to authors of this study which summarizes personal privacy cases resolved to date. The Ombudsman indicated to the authors of this study that material about the privacy cases could be published in this study as long as the parties were identified in an anonymous fashion (i.e., Mr. X and Ms. X).

⁹⁸ *Ibid.*

policy of obtaining customer consent; the complaint was resolved when the bank paid the customer \$500 for the privacy breach.

The Canadian Banking Ombudsman office also keeps statistics on the complaints received by internal bank ombudsmen and complaint officials. Most banks have now appointed ombudsmen or officials within the institution to investigate and resolve consumer complaints. These internal ombudsmen and officials resolve the large majority of complaints, given the relatively small number of complaints made to the Ombudsman. In July 1997, the Ombudsman's office released figures about complaints received by the 11 participating banks.⁹⁹ In the five-month period of the report, participating banks received 1,626 consumer complaints but only 1 per cent of the complaints related to privacy and confidentiality. Interviews by the authors of this study with several of the internal ombudsmen and officials confirmed that individual institutions are receiving a very low number of privacy complaints, generally in the range of one to a few per cent of all complaints.¹⁰⁰ All but a negligible number were quickly resolved to the satisfaction of the customer.

Insurance Industry Associations

Finally, the Canadian Life and Health Insurance Association Inc. and the Insurance Bureau of Canada run information centres which accept calls from consumers with questions about life and health insurance issues. Statistics about customer calls to these information centres show that only a small percentage relates to privacy. In the case of the CLHIA, of the 75,000 phone calls received in 1996, only 15 calls were identified as relating to privacy concerns.¹⁰¹ "Some increase in this number has been noted in recent years, perhaps arising from a general increase in awareness about privacy and increased publicity in this area, but the number of enquiries remains at a very modest level," the association has noted.¹⁰² In the case of the IBC, of the 113,000 consumer enquiries received by the IBC's five regional consumer information centres in 1997, only 342 related to privacy issues.¹⁰³ In general, these calls related to matters such as the right of an insurer to obtain a motor vehicle record, to obtain a previous accident history or to undertake surveillance of the insured when a claim for bodily injury has been made.

Significance of the Data

The foregoing sets out in some detail the types of complaints concerning privacy that are received; two observations should be considered here. First, the number of complaints, as

⁹⁹ See Canadian Banking Ombudsman, *supra*, note 96.

¹⁰⁰ In the Fall of 1997, we contacted bank ombudsmen or complaint officials at the following institutions: Canadian Imperial Bank of Commerce, Toronto-Dominion Bank, Canadian Western Bank, Bank of Nova Scotia, Laurentian Bank of Canada, Hongkong Bank of Canada, Citibank Canada, Bank of Montreal, National Bank of Canada, Amex Bank of Canada and Royal Bank. R.C. Owens and T.S. Onyshko met with, received phone calls from or received correspondence from most of these officials.

¹⁰¹ Canadian Life and Health Insurance Association Inc., *Privacy and Financial Institutions: Input to Mr. Owens and Mr. Wright re Task Force Research Project* (December 1997) at 5.

¹⁰² *Ibid.*

¹⁰³ Fax sent by Steven Lingard of the Insurance Bureau of Canada to T.S. Onyshko on May 22, 1998.

mentioned above, is extremely small compared to the number of transactions with individuals that such institutions engaged in on a regular basis. Large financial institutions have tens of thousands of employees and conduct hundreds of millions of customer transactions during a year. The relatively small number of complaints could be explained in part by the fact that individuals are not aware of the treatment of their personal information or of the correct body to which to make a complaint. But the negligible level of complaints compared to the numbers of transactions suggests that customers remain relatively satisfied with the manner in which privacy issues are addressed by financial institutions. Second, the particular complaints that have been made relate to incidents under varied and unique circumstances, which, while they may be of individual concern, do not support any reasonable conclusion of the widespread systemic failure of the existing forms of privacy protection.

One further note of caution is appropriate here. In compiling this study, we have spoken to industry participants, members of industry and consumer associations, reviewed documents on privacy and the financial services sector and considered anecdotal evidence relating to privacy issues. We have made every effort to properly document our observations and conclusions, but our empirical research necessarily has been limited by the reasonable deadlines and financial constraints imposed on the preparation of this study. While appropriate to our conclusions, our research is not meant to be presented as a comprehensive and statistically reliable consumer satisfaction survey.

Features of the Financial Services Sector in Canada

Before ending this introduction, it is necessary to discuss five characteristics of the financial services sector in Canada that have an impact on privacy issues. These characteristics provide important background to the observations and conclusions made in this study.

First, most financial institutions regulated by the federal government provide services across Canada. In general, these institutions may be regulated by the provinces and so will be affected by provincial laws; only banks are to a limited extent exempt from the application of provincial laws.¹⁰⁴ Financial services providers operating in Quebec may be bound by Quebec's privacy legislation relating to the private sector.¹⁰⁵ Likewise, insurers operating in Ontario would be bound by any future statute in that province which protects the privacy of medical information. Thus, there is the potential that a national institution will be caught in a patchwork of different provincial laws that set out different privacy standards. The situation becomes much worse if different provinces adopt conflicting or incompatible standards. In an ideal world, privacy regulation (actually, all regulation) for national financial services providers should be consistent across the country.

¹⁰⁴ For a further discussion of the provincial regulation of financial institutions and the exclusive federal jurisdiction over banks, see: Peter W. Hogg, *Constitutional Law of Canada*, Looseleaf edition, volume 1 (Scarborough, Ont.: Carswell, updated to 1997) at pp. 24-1ff.

¹⁰⁵ See, for example, Dubreuil, *supra*, note 50.

Second, privacy has been a part of the tradition of service offered by banks, trust companies, credit unions and insurers. In general, people feel comfortable providing details of their finances, income and health to financial institutions because they understand that such institutions can be trusted to keep information confidential. The culture of confidentiality that exists within these institutions has been bolstered by the common law's recognition that banks owe an implied duty of confidence.¹⁰⁶ Furthermore, a financial institution would have little to gain and much to lose by disclosing sensitive personal information to others. If these disclosures became public knowledge, customers would avoid the offending institution and seek out others which could be better trusted.

Third, the Canadian financial services sector has become increasingly competitive, in large part because of past reforms to the federal legislation governing financial institutions. In this competitive environment, financial institutions could be expected to address concerns about privacy as a means of attracting new customers and ensuring that existing customers remain loyal.

Fourth, Canadian financial services providers have made significant efforts to address privacy concerns. The insurance industry was one of the first to adopt industry codes to protect privacy in the early 1980s. More recently, banks and trust companies have adopted industry association privacy codes, in part in response to pressure from federal regulators. These codes generally follow the principles set out in the OECD guidelines and the CSA model code. In addition, the banking industry has established an ombudsman system to handle complaints about privacy and other matters. Customers unsatisfied by a particular bank's efforts to resolve a complaint may take the complaint to the office of the Canadian Banking Ombudsman. Particular codes may have shortcomings, and there are questions about the availability of the codes of some institutions to members of the public. However, these concerns should not obscure the fact that much progress has been made.

Fifth, there is a lack of hard evidence to suggest that privacy complaints are common in the financial services sector. For example, the statistics compiled by the Canadian Banking Ombudsman (and discussed at more length elsewhere in this Part) suggest that privacy complaints amount to about 1 per cent of all complaints received.¹⁰⁷ Given the lack of evidence of any widespread problem, legislators should be cautious when imposing new regulation.

The above characteristics suggest that policy makers should not rush to adopt new privacy legislation or regulation. In particular, there should be reasonable sensitivity to the costs that may be involved in new privacy measures. These costs include the costs of the financial institutions of complying with regulation (e.g., the costs of hiring and training additional personnel, printing costs, mailing costs, etc.) and the costs to the taxpayer of establishing a new system of regulation (e.g., the cost of assigning regulators to privacy matters).

¹⁰⁶ For further discussion of the common law implied duty of confidentiality, see Part II under the heading "The Implied Contractual Duty of Privacy".

¹⁰⁷ For further discussion of these statistics see this Part I under the heading "Public Concern About Privacy and Privacy Complaints".

Such costs will not cause an institution to fail and, in some instances, will overlap with costs that a reasonably prudent business would have had to incur to protect its customer data. But while these costs may not be material, they are significant in the sense that they represent a meaningful number of dollars. Thus, as a general approach, new privacy measures should be measured against both existing measures for privacy protection and the need for additional intervention.

II. Existing Privacy Protection

Introduction

Part II examines existing forms of privacy protection. The Part begins with a review of the way that common law and equity protect various aspects of privacy, as well as their shortcomings. It then discusses the banker's implied contractual duty of privacy, which was recognized in the seminal English case of *Tournier v. National Provincial & Union Bank of England*. Next, the Part considers the protection that existing federal and provincial legislation affords privacy. It reviews various provisions in federal laws governing banks, insurance companies, trust companies and credit associations and provincial laws that affect financial services providers and credit bureaux. It also reviews the provisions of Quebec's Act *respecting the protection of personal information in the private sector*, which represents Canada's first data protection statute applying to the private sector as a whole. Part II concludes with a lengthy review of the model privacy codes adopted by the industry associations for banks, trust companies and insurance companies and the model privacy code under consideration by the industry association for credit unions.

An Overview of Privacy at Common Law and Equity

No Canadian jurisdiction with the exception of Quebec has a general data protection statute which applies to the private sector. Individuals outside Quebec seeking a remedy for a perceived misuse of personal information must look to the common law or equity, a sector-specific federal or provincial statutory provision that relates to privacy matters, or the institution's own privacy code. This section briefly reviews certain relevant common law and equitable actions that protect aspects of privacy.¹⁰⁸ The application of contract law will be discussed in detail later in this Part, as well as specific federal and provincial statutory provisions, the Quebec privacy legislation and financial industry privacy codes.

The relevant torts and equitable actions may be broken down into two general categories: first, actions relating to intrusion into the individual's private life and, second, actions relating to the disclosure or use of personal information. Actions in the first category include trespass, nuisance and invasion of privacy, while actions in the second category include defamation, negligence, the rule in *Rylands v. Fletcher*, breach of confidence, and breach of fiduciary duty. However, when a contract forms the basis of the relationship between the parties, its provisions may restrict the ability of the parties to sue based on tort law or equity. As well, the implied contract between the parties has allowed courts to imply a legal duty of confidentiality into the relationship between the customer and his or her financial institution. As a result, contract law is particularly important in the context of the financial services industry.

¹⁰⁸ Please note that this section uses some material that first appeared in: Thomas Steven Onyshko, *Informational Privacy and the Law in Canada*, A Master of Laws Thesis (University of Toronto, Faculty of Law, Fall 1995).

Actions Relating to Intrusion

The tort of trespass is committed when there is physical interference with the individual's person, property or land. Historically, some cases have applied trespass to protect the plaintiff's privacy interest. For example, in *Sheen v. Clegg*¹⁰⁹ and *Grieg v. Grieg*,¹¹⁰ courts found that the defendants had committed trespass when they installed microphones in the homes of the plaintiffs. On the other hand, the taking of photographs by aerial surveillance has been found not to involve trespass, since there is no physical interference with the land.¹¹¹ In the context of financial institutions, if bank were to sift through an individual's safety deposit box without his or her permission, this might well constitute trespass.¹¹² In addition, one Ontario case suggests that the mailing of unsolicited marketing materials may amount to trespass when the material is physically delivered to the individual's home.¹¹³ However, this decision appears to fall outside the traditional scope of the tort.

The tort of nuisance protects the plaintiff's enjoyment or use of land. Traditionally, the action has been applied to recurrent intrusions, such as noises, smells and vibrations, which substantially and unreasonably interfere with the plaintiff's enjoyment of land. However, the Alberta Court of Appeal has held that harassment by telephone may be a nuisance if taken to an extreme. In *Motherwell v. Motherwell*,¹¹⁴ the court held that the tort was made out when the defendant made as many as 30 calls within the space of one hour to the plaintiff's home. Arguably, a telephone marketing campaign involving repeated phone calls might amount to nuisance.

The tort of invasion of privacy has been recognized in Ontario but is not well defined. The Ontario County Court first recognized the tort in *Saccone v. Orr*,¹¹⁵ when it awarded damages for the defendant's public use of a tape recording of a private conversation with the plaintiff. The

¹⁰⁹ Unreported. A description of the case appeared in the Daily Telegraph on June 22, 1961. See: Burns, "The Law and Privacy: The Canadian Experience" (1976) 54 *Canadian Bar Review* 1 at 13 footnote 85.

¹¹⁰ [1966] V.R. 376 (S.C.).

¹¹¹ *Bernstein of Leigh v. Skyviews & General Ltd.*, [1978] 1 Q.B. 479. See also *Malone v. Commissioner of Police (No. 2)*, [1979] 2 All E.R. 620 (Ch.D.), where the court found that government wiretapping of the plaintiff's telephone did not amount to trespass because it did not involve any act which physically intruded into the plaintiff's premises.

¹¹² It is unlikely that the institution's unauthorized use of personal information would be viewed as trespass on the individual's property. In order to show trespass, the customer would have to prove some proprietary interest in the personal information held by the bank and also some *physical* interference with his person or property.

¹¹³ In *Allan Mather v. Columbia House*, an unreported case decided August 6, 1992 by the Ontario Court (General Division), the plaintiff brought an action in contract against direct marketer Columbia House in an effort to get Columbia House to stop sending mail to his house. The plaintiff had repeatedly requested that he be removed from its mailing list but was unsuccessful. The court found that Columbia House had a duty not to forward junk mail to persons who specifically request that it not be done. In arriving at this conclusion the court made reference to the fact that Columbia House belonged to a national association and subscribed to a code of ethics that required them to delete names when requested to do so. The court held Columbia House liable for trespass and awarded the plaintiff general and punitive damages. The case is interesting for the court's willingness to stretch legal reasoning to find a remedy for a deeply annoyed homeowner, and for its suggestion that a voluntary code could be given legal effect.

¹¹⁴ [1976] 6 W.W.R. 550, 1 A.R. 47, 73 D.L.R. (3d) 62 (C.A.).

¹¹⁵ (1981), 34 O.R. (2d) 317.

tort was confirmed by two later decisions by Justice Mandel of the Ontario District Court and the Ontario Court (General Division).¹¹⁶ In *Palad v. Pantaleon*,¹¹⁷ Justice Mandel awarded \$2,500 for invasion of privacy in a case where a creditor had harassed a debtor by frequent phone calls and by appearing in the debtor's home and workplace. In *Roth v. Roth*,¹¹⁸ the judge awarded \$25,000 for mental distress as a result of invasion of privacy and \$5,000 in exemplary damages. One of the defendants in the case had assaulted one of the plaintiffs, removed articles from the plaintiffs' cottage and locked a gate leading to an access road to the cottage.

It is possible (but unlikely) that the privacy tort established by the Ontario decisions would apply to the collection and use of personal information. In theory, one might argue that the collection of personal information and use of information amounted to an invasion of privacy, particularly where the information was later used without the individual's knowledge or consent. But the Ontario cases have, in general, involved situations with an element of physical intrusion: for example, where the defendant physically invaded the privacy of the plaintiff's home, cottage or workplace. It is unclear whether the privacy tort is broad enough to apply to information. In the United States, where privacy jurisprudence is much better developed, the decision in *Dwyer v. American Express*,¹¹⁹ suggests that the U.S. tort of invasion of seclusion will not apply to the use of customer purchase information.

Actions Relating to the Disclosure or Use of Personal Information

The tort of defamation may provide a remedy if the defendant publishes (i.e., communicates to one or more other persons) confidential information about the plaintiff which is negative and wrong. To be considered defamatory, the statement must expose the plaintiff to hatred, contempt or ridicule, or tend to lower him or her in the eyes of reasonable members of society.¹²⁰ Defamation will only apply when the statement itself was false; thus, it will be available only when the defendant's conduct involved a mistake or some misconduct, and never when sensitive but true information is disclosed to a third party. In *Gillett v. Nissen*,¹²¹ the plaintiff sued his former employer after the former employer (falsely) told a potential new employer that the plaintiff had been dismissed for dishonesty. Similarly, an individual might sue a financial institution for releasing false credit information that reflected poorly on him or her. As an example, in *Cossette v. Dun*,¹²² the Supreme Court of Canada ruled that a Quebec company was

¹¹⁶ For further discussion of the development of the tort of invasion of privacy, see: Ian Lawson, *Privacy and Free Enterprise: The Legal Protection of Personal Information in the Private Sector* (Ottawa: Public Interest Advocacy Centre, 1992) at 226ff.

¹¹⁷ (14 June 1989), Ontario District Court, Action No. 266930/86 (unreported).

¹¹⁸ (1991), 4 O.R. (3d) 740 (O.C.G.D.).

¹¹⁹ 652 N.E. 2d 1351 (1995, Ill. App. Ct.). In *Dwyer*, several American Express cardholders claimed that the company's practice of selling information about consumer purchases amounted to invasion of seclusion. The Illinois Court of Appeals dismissed the action. The court noted that use of the credit card was voluntary and that the company's practice resembled the sale of magazine subscription lists, which had been upheld by other U.S. case law.

¹²⁰ For a general discussion on the law of defamation, see Raymond E. Brown, *The Law of Defamation in Canada*, vol. I (Toronto: Carswell, 1994) at 1-16.1ff.

¹²¹ (1976), 58 D.L.R. (3d) 104 (Alta. S.C.).

¹²² (1891), 18 S.C.R. 22.

liable for damages for a false credit report that brought the plaintiff to the brink of financial ruin.¹²³

The rule in *Rylands v. Fletcher* provides a remedy for harm caused by the release of certain dangerous or noxious substances. In *Rylands v. Fletcher*¹²⁴, the House of Lords found that the defendant factory owner was strictly liable when a reservoir maintained on its property burst into the plaintiff's neighbouring coal mine causing damage to the plaintiff's property. The English courts imposed strict liability on the principle that a "person who for his own purposes brings onto his own lands and collects and keeps there anything likely to do mischief if it escapes, must keep it at his peril, and, if he does not do so, is prima facie answerable for all the damage which is the natural consequence of its escape."¹²⁵ Some Canadian observers have argued that the rule in *Rylands v. Fletcher* might apply to databases of sensitive information, so that the controller of the database would be strictly liable for the harm caused by unauthorized use or disclosure of such information.¹²⁶ Thus, an individual harmed by the unauthorized release of financial information from the data bank of a financial institution might sue based on this rule. However, it is unclear whether the rule could be stretched so far from its roots that it would cover personal information stored in databanks. Case law under the rule has dealt with the escape of physical objects, fire and vibrations; it might be difficult to argue that the escape of something as intangible as information should be treated in the same way.

The equitable action of breach of confidence may provide a remedy for the unauthorized use or disclosure of the plaintiff's information. The action applies when three requirements are met: first, the information must have the necessary character of confidentiality; second, communication of the information must occur in circumstances giving rise to an obligation of confidence; and, third, there must be mis-use or unauthorized use of the information.¹²⁷ It appears that both common law and equitable remedies will be available to the successful plaintiff.¹²⁸ The main Canadian cases to date have involved commercial information,¹²⁹ but a handful of English cases have used the action to protect types of personal information. For

¹²³ Mr. Justice Ritchie of the court stressed the need for reporting companies to make reasonable efforts to ascertain the truth of credit information, given that individuals had no right of access to their own files. (The case was decided in 1891, long before provincial credit reporting laws which give individuals a right of access to their own information.) However, *Cossette v. Dun* was decided under the principle of tortious liability set out in the Quebec Civil Code, so that the court did not consider general common law principles relating to defamation.

¹²⁴ (1866) L.R. 1 Ex 265, aff'd (1868) L.R. 3 H.L. 330.

¹²⁵ (1866) L.R. 1 Ex 265 at 279-280. Recently, the House of Lords confirmed that the foreseeability principle applied to the rule so that the defendant will not be liable for the spill of material which was not known to be hazardous at the time of the spill: *Cambridge Water Company v. Eastern Counties Leather*, [1994] 1 All E.R. 53.

¹²⁶ See: Dale Gibson, "Regulating the Personal Reporting Industry," in *Aspects of Privacy Law: Essays in Honour of John M. Sharp*, ed. by Dale Gibson (Toronto: Butterworths, 1980) 111 at 127; and Chris Dockrill, "Computer Data Banks and Personal Information: Protection Against Negligent Disclosure," (1988) 11 *Dalhousie Law Journal* 546 at 564-566.

¹²⁷ See: Mistrale Goudreau, "Protecting Ideas and Information in Common Law Canada and Quebec," (1994) 8 *Intellectual Property Journal* 189 at 192.

¹²⁸ See, for example, Mr. Justice Sopinka's comments in *LAC Minerals v. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574 at 615.

¹²⁹ *LAC Minerals v. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574; *Pharand Ski Corporation v. Alberta* (1991), 7 C.C.L.T. 225 (Alta. Q.B.).

example, in *Duchess of Argyll v. Duke of Argyll*,¹³⁰ the court issued an injunction to prevent the Duke of Argyll from publishing confidences of his former Duchess although she had since divorced him. And in *X. v. Y.*,¹³¹ the court issued an injunction to prevent a newspaper from publishing the names of two doctors who had contracted AIDS. If a financial institution proposed to make some unauthorized use of personal information, an action for breach of confidence might be available depending on the nature of the information and the circumstances under which it was communicated to the institution.

Finally, the equitable action of breach of fiduciary duty may prevent the unauthorized use of information in certain relationships. In general, fiduciary duties apply to the dominant party in a relationship with a special element of trust or authority, such as the relationship between solicitor and client or doctor and patient.¹³² In addition, courts have been willing to impose duties on parties outside the traditional trust relationships, based on the particular facts of the case.¹³³ Fiduciary duties require the fiduciary to act with good faith towards the beneficiary; as a result, the fiduciary is prohibited from using information communicated within the relationship for an unauthorized purpose. It is possible that, in certain circumstances, a bank, insurer, trust company, or credit union will be recognized as being in a fiduciary relationship with an individual.

Contract Law

Contract law provides a double-edged sword that may be wielded both to protect and diminish privacy interests. On the one hand, express or implied terms in the contract may protect the confidentiality of information and the customer's privacy interest. On the other hand, the express terms of a contract may limit the scope of privacy protection that a customer would otherwise enjoy.

Contract law is particularly important in the case of financial institutions. Based on the English Court of Appeal's decision in *Tournier*,¹³⁴ courts have recognized that a duty of confidentiality should be an implied term of the contract between the banker and the customer. This implied duty of confidentiality may place important limits on the activities of the financial institution, unless it is modified by express contractual terms. In addition, it is possible that the terms of an

¹³⁰ [1967], Ch.D. 302.

¹³¹ [1988], 2 All E.R. 648.

¹³² For a general discussion of the law of fiduciary duties, see: *Special Lectures of the Law Society of Upper Canada, 1991: Fiduciary Duties* (Toronto: Richard De Boo, 1991).

¹³³ The general test that has been adopted by various members of the Supreme Court of Canada was first proposed by Madam Justice Wilson in *Framé v. Smith*, [1987] 2 S.C.R. 99 at 135-136. This test suggests that fiduciary obligations will be imposed on parties in relationships that possess three general characteristics: "(1) The fiduciary has scope for the exercise of some discretion or power. (2) The fiduciary can unilaterally exercise that power or discretion so as to affect the fiduciary's legal or practical interests. (3) The beneficiary is particularly vulnerable to or at the mercy of the fiduciary holding the discretion or power." See: *LAC Minerals v. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574 at 599, per Sopinka J. Note, however, that judges have stressed that fiduciary duties will be imposed in a flexible fashion and that a relationship may be fiduciary for some purposes and not for others. See: *LAC Minerals v. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574 at 648, per La Forest, J.

¹³⁴ [1924], 1 K.B. 461 (C.A.).

institution's privacy code form an implied part of the customer's contract with the institution, so that a breach of the privacy code may be a breach of the contract. (The *Tournier* case and the possibility that privacy code terms will be implied into the customer's contract will be discussed in more detail below.)¹³⁵

However, contracts between financial institutions and their customers usually include provisions which effect consent, as required by privacy codes, to certain uses of personal information. Such terms usually take the form of a list of third parties from whom the institution may gather personal information about the individual, or a list of third parties to whom the institution may provide personal information about the individual. In some cases, these provisions appear excessively broad. It is worth examining provisions that appear in the form used to open accounts with several banks. (The reference to bank forms is convenient and illustrative, but we do not mean to single out the banks; similar provisions appear in contracts with insurers, trust and security dealers.) The Bank of Nova Scotia application for deposit services states on its back:

Scotiabank collects information from you for the purposes of establishing and maintaining a relationship, offering and providing products and services, rendering credit decisions, marketing services, complying with the law, protecting your and the Bank's interests and for any other compatible purpose.

By signing on the front of this Application, you confirm that the information you have given is true and complete. You authorize us to give to, obtain, verify, share and exchange credit and other information about you with others, including credit bureaux and any subsidiary of the Bank as well as any other person with whom you have financial dealings or as may be otherwise permitted or required by law. You also authorize any person whom we contact in this regard to provide such information. You authorize us to send you information about products of the Bank and its subsidiaries and agree that we may use the information about you for marketing purposes after the relationship created by this agreement has ended.¹³⁶

The Canadian Imperial Bank of Commerce account and services application form states above the signature line:

You may, from time to time, give any credit and other information about me, including any information on this form, to, and receive such information from, any: (a) credit bureau or reporting agency; (b) person with whom I may have or propose to have financial dealings; and (c) person in connection with any dealings I have or propose to have with you. I agree that you may use that information to establish and maintain my relationship with you, and to offer me any services from time to time, as permitted by law.¹³⁷

¹³⁵ For further discussion of *Tournier* and privacy codes, see the discussion in this Part II under the heading The Implied Contractual Duty of Privacy.

¹³⁶ Bank of Nova Scotia, *Application for Deposit Services* (Form), apparently dated "9/96" and obtained from Scotiabank branch in downtown Toronto in Fall 1997. It should be noted that the form refers to a *Personal Banking Agreement* Booklet; a review of the booklet confirms that it does not contain additional provisions that affect privacy.

¹³⁷ Canadian Imperial Bank of Commerce, *Personal Account and Services Application – Account Information* (Form), apparently dated "95/08" and obtained from a branch of the CIBC in downtown Toronto in Fall 1997.

The Toronto Dominion-Bank financial services agreement form states above the signature line:

You authorize us to obtain credit or other information about you, to the extent permitted by law. We can give other credit grantors and credit bureaus information about your application and your credit experience with us.¹³⁸

Royal Bank's application for a personal deposit account states on the second page of the form above the signature line:

You may collect credit and other financially-related information about me ("Information") from me, from service arrangements I have made with or through you, from credit bureaux and other financial institutions, and from references I have provided to you. You may give Information to credit bureaux and other financial institutions and, with my consent, to other parties. You may also use Information to determine my financial situation and keep it in your records so long as it is needed for the purposes described above.¹³⁹

In addition, a Royal Bank client agreement form associated with the application form contains detailed provisions on the collection and use of personal information:

From time to time,

- (a) You may collect credit and other financially-related information about me ("Information") from me, from service arrangements I have made with or through you, from credit bureaux and from other financial institutions, and from references I have provided to you;**
- (b) You may use Information as follows:**
 - (i) You may give it to credit bureaux and other financial institutions and, with my consent, to other parties,**
 - (ii) You may use it to determine my financial situation,**
 - (iii) You may use it for any purpose related to the provision to me of services I request from you. You may also give it to anyone who works with or for you, but only as needed for the provision of those services,**
 - (iv) You may use my social insurance number for income tax reporting purposes if I have given that number to you; and**
- (c) You may also use information for the following purposes:**
 - (i) You may use it to promote your services to me. You may also add it to client lists you prepare and use for this purpose,**
 - (ii) You may share it with other members of Royal Bank Financial Group (where the law allows this) so that they may promote their services to me, and**

¹³⁸ Toronto-Dominion Bank, *Financial Services Agreement* (Form), apparently dated "6-95" and obtained from a branch of the TD Bank in downtown Toronto in Fall 1997.

¹³⁹ Royal Bank, *Application for Personal Deposit Account* (Form), apparently dated "10-1997" and obtained from a branch of Royal Bank in downtown Toronto in Fall 1997.

- (iii) You may also use my social insurance number as an aid to identify me with credit bureaux and other financial institutions for credit history file matching purposes.

I may tell you to stop using Information in the ways described in (c) at any time by contacting my branch or by calling you toll-free at 1-800 ROYAL 9-9.

You acknowledge that the use of Information in the ways described in (c) is at my option and that I will not be refused credit or other services just because I have told you to stop using it in those ways.

For the purposes of (c)(ii), other members of Royal Bank Financial Group include your affiliates which are engaged in the business of providing any one or more of the following services to the public in Canada: deposits, loans and other personal financial services; credit, charge and payment card services; trust and custodial services; securities and brokerage services; insurance services.

If I am no longer your client or this Agreement terminates, you may keep information in your records so long as it is needed for the purposes described in (b) above.¹⁴⁰

A review of the forms suggests that, in general, they provide a wide scope for both the collection and disclosure of personal information.

In general, the bank forms discussed above raise certain concerns about the use of contractual provisions to authorize the collection and disclosure of personal information. (As a separate but similar example, the insurance claim forms used by insurance companies may provide very wide powers of collection and disclosure to the insurance company.¹⁴¹) As noted above, the forms often give very wide powers of collection and disclosure to the bank – to the point where they could undermine effective privacy protection. Moreover, a power imbalance exists between the bank and the individual customer. An individual bank customer confronted with a standard corporate form will not have the ability to propose changes to the form that better protect his or her privacy. The bank simply will not accept changes to the standard form used for consumer transactions. In addition, individuals may not be aware of the differences between different banks' standard forms; in any case, such forms generally take the same approach. In defence of the banks, it is understandable why, from a legal perspective, such consent would be drafted very broadly. It is difficult to anticipate every legitimate need to share information and lawyers tend to draft broadly, particularly when there is no negotiation to force them into a narrower approach. In part because the bank forms are not negotiated, there will be a tendency on the part of the courts to interpret them against the banks. For instance, while the Bank of Nova Scotia account form appears on its face to be broad enough to permit virtually any information sharing, there is little chance that a court would permit reliance on such a clause in cases that fell outside the scope of what the customer would reasonably have anticipated when signing the form.

¹⁴⁰ Royal Bank, *Client Agreement* (Form), apparently dated "11-96" and obtained from a branch of Royal Bank in downtown Toronto in Fall 1997.

¹⁴¹ Several complaints to the Quebec privacy commission have led to findings that the provisions of insurance company forms are much broader than necessary in the circumstances. For further discussion of these complaints, see Part I under the heading Public Concern About Privacy and Privacy Complaints.

The above discussion reflects the limitations of contract law to protect privacy. However, it also reflects the reality of the provision of services on the mass scale that banks and insurance companies provide. The inefficiencies caused, and the costs to both institution and customer imposed, by negotiation of every contract between them, would put such services out of the reach of virtually all consumers. Therefore, contract, like the enforcement mechanism of suing in court, ought not to be seen as a comprehensive form of privacy protection.

General Shortcomings of Common Law and Equitable Actions

Tort law, equity and contract law may protect various aspects of privacy. However, two general shortcomings of legal and equitable actions should also be considered. First, in many cases it may be difficult to show that the plaintiff has suffered significant damages as a result of the unauthorized disclosure or mis-use of personal information.¹⁴² If the plaintiff cannot show actual damages, the action will be dismissed or the plaintiff will receive only nominal damages depending on the nature of the particular action involved. This may be just in the circumstances, but it does little to enforce a standard of conduct. Second, the high cost of bringing a court action will discourage many individuals from seeking a common law or equitable remedy for a privacy problem. Disclosure or mis-use of personal information often will involve small amounts of provable damages, yet the individual must pay significant legal fees in order to bring an action.

The Implied Contractual Duty of Privacy

Tournier and the Implied Duty of Confidentiality

Common law decisions have established that an implied contractual duty of confidentiality applies to the relationship between a bank and its customers. By extension, a similar duty should apply to the relationships between other financial institutions and their customers. The common law duty will have an important effect on the way that financial institutions treat information relating to their customers. As a result of the duty, financial institutions may be more restricted than other corporations in their ability to disclose personal information to third parties.

The implied duty of confidentiality was recognized by the leading English case of *Tournier v. National Provincial & Union Bank of England*.¹⁴³ In the case, a bank disclosed information about one of its customers, Mr. Tournier, to his employer. In particular, the bank disclosed the fact that Mr. Tournier made frequent overdrafts and that he had endorsed a cheque in the name of a bookmaker. When Mr. Tournier was not hired at the end of his probationary term, he brought an action against the bank. He alleged that an implied contractual term prevented the bank from disclosing information about his account to third parties.

¹⁴² See, for example, the defamation case of *Gillett v. Nissen* (1976), 58 D.L.R. (3d) 104 (Alta. S.C.). There, the plaintiff failed to receive a job from a new employer after his former employer made false statements about his honesty; however, the plaintiff was unable to show that the statements were the cause of his not receiving the job.

¹⁴³ [1924] 1 K.B. 461 (C.A.).

The English Court of Appeal held that there was no contractual requirement of absolute confidentiality between a bank and its customers. However, it found that there was an implied term of the banker-customer contract which required that customer information be kept confidential, subject to four qualifications. The three-judge panel of the court declined to provide a complete definition of the bank's positive duty but discussed the scope, timing and qualifications which applied to the duty.

On the timing and scope of the duty of confidentiality, Justice Banks of the court took the position that:¹⁴⁴

- the duty did not end when the account closed, so that information about the account remained confidential unless it could be released under one of the qualifications;
- information considered confidential was not limited to the state of the account but included any information gained from the account itself, such as the customer's address and other personal information; and
- the duty did not extend only to information derived from the customer alone but extended to information derived about the customer from other sources, provided it was gathered by bank personnel in their capacity as bank representatives.

Justice Banks then set out four qualifications to the implied duty of confidentiality, which remain relevant today. He found that a bank could disclose customer information:

- where the disclosure was under compulsion by law;
- where there was a duty to the public to disclose;
- where the interests of the bank required disclosure; and
- where the disclosure was made with the express or implied consent of the customer.

The implied duty of confidentiality recognized in *Tournier* has been applied and interpreted by cases in England, Canada, the United States and other Commonwealth countries.¹⁴⁵ For

¹⁴⁴ The three appeal judges produced different reasons, although Banks' reasons are often cited in later cases. Because of the different sets of reasons, the precise scope of the implied duty of confidentiality recognized by *Tournier* is not as clear as one might like and, in fact, one judge took a much narrower view of the duty. While Banks, J. and Atkin, J. held that the duty extended to all information collected from or arising out of the relationship of banker and customer, Scrutton, J. suggested that the duty applied to the customer's account and related transaction but not to information derived from other sources. And, while Banks, J. and Atkin J. were of the view that the duty would not come to an end when the account was closed, Scrutton J. took the position that the duty did not apply to information acquired before or after the existence of contractual relations between the bank and its customer.

example, in *Hull v. Childs & Huron and Erie Mortgage Corp.*, the Ontario High Court held that disclosure of the amount of a customer's credit to a third party would constitute breach of the implied duty, even where that person presented a blank cheque purporting to authorize the payee to withdraw the entire balance in the account.¹⁴⁶ And, in *Guertin v. Royal Bank of Canada*, the Ontario High Court held that the duty not to disclose confidential customer information also encompassed a duty on the part of bank employees not to use such information for their own advantage.¹⁴⁷ Other decisions have suggested that disclosure of confidential information by one entity to another within a structure of holding companies and subsidiaries may constitute a breach of the duty.¹⁴⁸

Case law has also interpreted the scope of the four exceptions to the duty of confidentiality set out by Justice Banks. The first exception applies when the disclosure of information is compelled in the course of legal proceedings by law or by court order.¹⁴⁹ Such disclosure also may be required in order to comply with statutory provisions of both Canadian and foreign law.¹⁵⁰ Where a bank is compelled to make disclosure in connection with legal proceedings, it should make reasonable attempts to inform the customer that this will be necessary, although

¹⁴⁵ *Tournier* was recently affirmed in a decision of the Judicial Committee of the English Privy Council, *Robertson v. Canadian Imperial Bank of Commerce*, [1995] 1 All E.R. 824 (P.C.). For Australian cases, see *Smorgen v. Australia and New Zealand Banking Group Ltd* (1976), 134 C.L.R. 475; *Re Peter Lawrence Crawley et al* (1981), 52 F.L.R. 123; *Re Kingston Thoroughbred Horse Stud and Australian Tax Office No. N85/130* (1986) (Administrative Appeals Tribunal); *Kabwand Pty. Ltd. v. National Australian Bank Limited* (1989), No. G355, Fed. No. 195 (Aust. F.C.); *Australian Securities Commission v. Westpac Banking Corporation* (1991), A.C.S.R. 350, 32 F.C.R. 546. For United States cases, see *Jacobsen v. Citizens State Bank* (1979), 587 SW2d 480 (Tex. Civ. App.); *Suburban Trust Co.* (1979), 408 A.2d at 758; *State v. McCray* (1976) 15 Wash. App. 810, 551 P.2d 1376; *Burrows v. Superior Court of San Bernardino County* (1974), 13 Cal. 3d 238, 118 Cal. Rptr. 166, 529 P.2d 590; *Pigg v. Robertson* (1977), 549 SW2d 597; *Taylor v. Commerical Bank* (1903) 174 NY 181, 66 NE 726.

¹⁴⁶ *Hull v. Childs & Huron and Erie Mortgage Corp.*, [1951] O.W.N. 116.

¹⁴⁷ (1983), 43 O.R. (2d) 363 at 374. See also the recent case of *Hongkong Bank of Canada v. Phillips*, [1997] M.J. No. 134 (Man. Q.B.), where the Manitoba Court of Queen's Bench held that a bank's duty of confidentiality to one customer did not obviate the "minimal duty of the bank" to advise another customer to seek independent legal or financial advice with respect to a transaction involving risks of which the bank was well aware.

¹⁴⁸ [1987] A.C. 45 at 53-54, [1986] 3 All E.R. 468 at 475-476 (C.A.); *Bhogal v. Punjab National Bank*, [1988] 2 All E.R. 296 at 305 (C.A.).

¹⁴⁹ See Bradley Crawford, *Crawford and Falconbridge on Banking and Bills of Exchange*, 8th ed. (Toronto, 1989) at 806-811. Canadian law does not recognize an inherent privilege in banking information: see, for example, *R. v. Spencer* (1983), 2 C.C.C. (3d) 526 (C.A.), per McKinnon A.C.J.O. In *Haughton v. Haughton*, [1965] 1 O.R. 481, the court held that a subpoena was insufficient to compel a bank manager to testify but that a specific court order would constitute the requisite "compulsion of law" to override the banker's duty of confidentiality. *Haughton* was later affirmed in *Royal Bank of Canada v. Art's Welding & Machine Shop* (1989), 34 C.P.C. (2d) 190.

¹⁵⁰ See *CIBC v. A.-G. Can.* (1962), 35 D.L.R. (2d) 49 (S.C.C.); and Rosemary Regan, "You Don't Say," (1982) 89 *Canadian Banker* 32. See also *Budzich v. Toronto Dominion Bank*, [1996] 2 C.T.C. 278, where the parties conceded that a demand by Revenue Canada pursuant to a statutory power constituted a "compulsion of law"; and *Park v. Bank of Montreal*, [1997] B.C.J. No. 787, where the court found that a bank's disclosure through its Korean Branch to the Korean criminal prosecutor's office constituted a compulsion of law because the disclosure was required under Korean law.

there is no absolute duty to do so given the difficulty a bank may have in actually reaching a customer in the time available.¹⁵¹

The second exception applies when disclosure arises as a matter of public duty.¹⁵² It has been suggested that the exception might apply if a bank disclosed information to the authorities about a customer suspected of criminal activity, or trading with the enemy during wartime. However, there have been few actual instances where this exception has been invoked.¹⁵³ In *R. v. Lillico*, disclosure of customer information to the police for the purposes of a criminal investigation into the acts of the customer was justified on the grounds of public interest.¹⁵⁴ It was also held in *Lillico* that while there is an inherent privacy interest in information, which may attract the protection of s. 8 of the *Canadian Charter of Rights and Freedoms*, the public interest in effective law enforcement through the disclosure of general banking information (e.g., confirmation that a particular cheque was deposited in the customer's account) outweighed any infringement of the customer's privacy that would attract the protection of s. 8 of the *Charter*.¹⁵⁵ Although a bank may be required to disclose customer information for the purpose of a criminal investigation, disclosure by a bank that a customer is generally a "dishonest" person will not be justified by a duty to the public.¹⁵⁶

The third exception applies when the interests of the bank may justify the disclosure of confidential information, as when the bank sues for settlement of an overdrawn account or seeks to protect itself against fraud or crime.¹⁵⁷ Disclosure must be reasonably necessary for the protection of the bank's interests, and presumably is not permitted where it is merely to the

¹⁵¹ *Robertson v. Canadian Imperial Bank of Commerce*, *supra*, note 145, *per* Lord Nolan. There may also be situations in which a bank may be entitled to refrain from informing the customer, which would arise by implied agreement and on the grounds of protecting the bank's own interest or as a result of public duty: see *ibid.*; *X A.-G. v. A Bank*, [1983] 2 All E.R. 464; and *Marcel v. Commissioner of Police of the Metropolis*, [1992] 1 All E.R. 72, Ch. 225. Canadian cases have also considered this issue. See *Budzich v. Toronto Dominion Bank*, [1996] 2 C.T.C. 278, where the *Robertson* decision was considered, and the court suggested that a bank may have a duty to warn a customer when it has been compelled by Revenue Canada to disclose the customer's information; and *Foundation Co. of Canada Ltd. v. Dhillon*, [1995] O.J. 3211 (Ont. Ct. Gen. Div.), where the court stated that there was no duty to warn where there existed a *prima facie* case that the customer had breached a trust, committed fraud, and accepted secret commissions. See also *Park v. Bank of Montreal*, [1997] B.C.J. No. 787, where the court held that when the compulsion is in relation to a non-criminal matter, there is ordinarily a duty on the bank to use its best efforts to warn the customer of the disclosure. However, where the disclosure is in relation to an alleged criminal activity, there is no implied term that the bank should first warn the customer.

¹⁵² *Tournier*, *supra*, note 143 at 473. See also *Weld-Blundell v. Stephens*, [1920] A.C. 956 at 965.

¹⁵³ *Crawford & Falconbridge*, *supra*, note 149, at 811. See, for example, *Libyan Arab Foreign Bank v. Bankers Trust Co.*, [1988] 1 Lloyd's Rep. 259.

¹⁵⁴ (1994), 92 C.C.C. (3d) 90 (Ont. Ct. Gen. Div.).

¹⁵⁵ *Ibid.*, at 93-94 and 95.

¹⁵⁶ *Murano v. Bank of Montreal* (1995), 31 C.B.R. (3d) 1, 20 B.L.R. (2d) 61, where the court rejected the argument that the disclosure by the bank to a customer's business associates, suppliers and other lenders that the customer was "dishonest" was justified by a duty to the public. But see also *Canada Deposit Insurance Corp. v. Canadian Commercial Bank* (1989), 64 Alta. L.R. (2d) 329, 71 C.B.R. (N.S.) 239, 95 A.R. 24, A.W.L.D. 367, where the court held that because the Canadian Deposit Insurance Corporation needed to inspect bank accounts in the custody of the liquidator, there existed a "higher duty to the public that requires disclosure on a broader basis than would be obtainable by way of [documentary discovery]."

¹⁵⁷ *Tournier*, *supra*, note 143 at 473, *per* Banks L.J.; at 481, *per* Scrutton L.J.; at 486, *per* Atkin L.J.

bank's advantage to disclose the information.¹⁵⁸ *Montgomery v. Ryan* provides an example of this sort of disclosure; there, the bank was justified in revealing the particulars of the indebtedness represented by a note, and of the collateral securing it, to a potential purchaser.¹⁵⁹ In *Canadian Imperial Bank of Commerce v. Sayani*, the British Columbia Court of Appeal found that it is "inconceivable that an honest banker would ever be willing to do business on terms obliging the bank to remain silent in order to facilitate its customer in deceiving a third party."¹⁶⁰ And in *Sutherland v. Barclays Bank Ltd.*, the defendant bank was held to have acted properly in its own interest in disclosing to the husband of the plaintiff that she was overdrawn and that most of the cheques passing through her account were in favour of her bookmakers.¹⁶¹

The final exception applies when the customer consents to the disclosure, either expressly or by implication.¹⁶² The most common occasion where this occurs in a banking setting is where the customer authorizes disclosure to a third party for the purpose of credit reporting. While circumstances involving express authorization from the customer are relatively straightforward, questions of implied consent have been more difficult for the courts to resolve. Canadian courts have held that a signed blank cheque does not itself imply the signatory's consent to disclose confidential information to third parties.¹⁶³ On the other hand, in *Royal Bank of Canada v. Art's Welding & Machine Shop*, the court was willing to find that where a customer knew that another party's livelihood depended on their contractual relations, this implied the customer's consent for the bank to disclose his records to the other party.¹⁶⁴ It should also be noted that while the duty of confidentiality will not apply to information so disclosed, the bank might still be liable in tort should the disclosure cause economic loss.¹⁶⁵

The *Tournier* decision provides a basic confidentiality framework which restricts the ability of banks – and, by implication, other financial institutions – to disclose information to third parties. However, it does not address all issues relating to personal information. For example, the decision does not restrict the type of information that may be collected about a customer. It has nothing to say about when (if it all) a bank reaches the point where it passes beyond the scope of legitimate inquiry when it collects information from its customers. The decision does not govern

¹⁵⁸ *Ibid.*, at 481, *per* Scrutton L.J.; at 486, *per* Atkin L.J. Also, in *Park v. Bank of Montreal*, [1997] B.C.J. No. 787, the court stated that this exception to the duty of confidentiality "should be construed narrowly"; but in *Royal Bank of Canada v. Brattberg* (1993), 11 Alta. L.R. (3d) 190, 8 W.W.R. 139, 143 A.R. 131, A.W.L.D. 684, the bank was entitled to disclose the fact that it held a security interest in the customer's property in order to protect that interest. See also *Crawford & Falconbridge*, *supra*, note 149 at 812-814.

¹⁵⁹ (1907), 9 O.W.R. 572 (H.C.), *rev'd* (1908), 16 O.L.R. 75 (C.A.).

¹⁶⁰ (1993), 83 B.C.L.R. (2d) 167 at 172, *per* Taylor J.A.

¹⁶¹ (1938) 5 L.D.A.B. 163, *per* Du Parcq L.J. His Lordship also held that the plaintiff had given her implied consent to the disclosure.

¹⁶² *Tournier*, *supra*, note 143 at 473, *per* Bankes L.J. Whether a customer has consented is a question of fact: *ibid.*, at 468, *per* Atkin L.J.

¹⁶³ See *Hull v. Childs*, *supra*, note 146.

¹⁶⁴ *Royal Bank of Canada v. Art's Welding & Machine Shop*, (1989), 34 C.P.C. (2d) 190, A.W.L.D. 653, C.L.D. 895. See also *Hong Kong Bank of Canada v. Phillips*, [1997] M.J. No. 134 (Man. Q.B.), where a customer who brought in new clients to a bank to which he was in arrears so that those clients could borrow money to invest in his ventures, was held to have impliedly consented to the bank disclosing the information he had given it with respect to those ventures.

¹⁶⁵ See *supra*, note 150.

the way a bank itself uses personal information collected from or about a customer. It would not stop a bank from taking information collected for one purpose and using it for another purpose (e.g., the marketing of an unrelated bank service). And the decision does not establish any right of access to personal information, or a right to seek a correction of personal information which is inaccurate. Yet principles limiting the collection, use or disclosure of personal information and establishing access rights to such information have become integral aspects of modern privacy protection.

Implied Terms and Privacy Codes

It is possible that the voluntary codes of privacy that many financial institutions have publicly adopted may be viewed as implied terms in contractual agreements between these institutions and their customers. Under common law doctrine, a court may imply a term into a contract to give efficacy to a contractual relationship¹⁶⁶ or because trade custom or general business practice¹⁶⁷ dictate that such a term is understood to be included in the contract. However, if the courts were willing to treat the provisions of a privacy code as implied contractual terms, an individual would still have to prove the breach of his contractual right and make the case for a remedy such as damages or specific performance. Moreover, a contract signed by the customer that contained a specific clause consenting to the transfer or other use of personal information likely would prevail over any general privacy provisions in the code. Hence, the provisions of a privacy code are best enforced through a more flexible complaints process, such as the bank ombudsman.

It is debatable whether the terms of the financial institution's privacy code would be necessary in order to give efficacy to the contractual relationship with the customer. As Professor G.H.L. Fridman has written on the notion of business efficacy: "The theory behind this doctrine is that had the 'officious bystander' drawn the attention of the parties to the matter in issue, they would have agreed that the contract should provide for its resolution in the manner which is subsequently suggested, in later litigation, as the implied term."¹⁶⁸ Had the officious bystander drawn the institution's privacy code to the attention of the customer at the time that the customer entered the contract with the institution, the customer might well have viewed the terms of the code as part of the contract. On the other hand, the financial institution would have a different view of the matter. As well, one may argue that the terms of a privacy code are not essential to the operation of the contract since many such contracts were entered into before Canadian financial institutions adopted privacy codes.

¹⁶⁶ "The law is very clear that where it is reasonably necessary, having regard to the circumstances or where there is an operative business practice that may be said to govern the relationship of the parties, a term may be implied to give efficacy to the contractual relationship." See: *Midland Doherty Limited v. Rohrer* (1984), 62 N.S.R. (2d) 205 at 212 (N.S.T.D.).

¹⁶⁷ "Usage, of course, where it is established, may annex an unexpressed incident to a written contract; but it must be reasonably certain and so notorious and so generally acquiesced in that it may be presumed to form an ingredient of the contract." See: *Georgia Construction Co. v. Pacific Great Eastern R. Co.*, [1929] 4 D.L.R. 161 at 163 (S.C.C.).

¹⁶⁸ See: G.H.L. Fridman, *The Law of Contract in Canada*, 3rd ed. (Scarborough: Carswell, 1994) at 476.

In addition, courts may recognize an implied term based on a widely accepted usage or custom in the trade, business, or profession. The courts have, however, been fairly strict in their recognition of implied terms on this basis; the usage must be “so generally acquiesced” by those in the business that it can be “presumed to form an ingredient of the contract.”¹⁶⁹ It is possible that the Canadian Bankers Association’s model privacy code would meet this threshold. The Code has been in effect in one form or another since 1990 and has been promoted by the banking association to the public and government officials as the industry’s response to privacy concerns. As well, the Code often uses mandatory language relating to a bank’s privacy duties. These facts might tend to support a conclusion that the Code has been generally acquiesced to by the banking industry.

There is little Canadian case law that deals specifically with the issue of imposing the terms of a voluntary code into a contractual agreement.¹⁷⁰ In *Banks v. Biensch*,¹⁷¹ the court considered a “Code of Ethics” published by a Charolais bull and cow breeders association which guaranteed animals sold would be breeders. The court determined that the usage of the trade in sales of Charolais animals by members of the association was so well recognized and established that the Code could be assumed as implied terms of sale. In *Smith v. Kamloops and District Elizabeth Fry Society*,¹⁷² a social worker was dismissed because of her relationship with a client who was receiving counseling at the Society. The action for wrongful dismissal was dismissed on the ground that there was an implied term of the plaintiff’s employment contract that she abide by the British Columbia Association of Social Workers’ Code of Ethics. These two cases lend some support to the proposition that privacy codes may be treated as implied contractual terms. As well, it seems likely that as the public becomes more aware of these codes, the argument for deeming the codes’ provisions to be implied terms will become stronger.

The difficulties with the implied term analysis can be avoided to a large extent since, arguably, the financial institutions are holding out privacy codes as governing the relationship with the customer, and as therefore being express contract terms. Whether or not this is the case might depend upon agreements the customer had signed with the financial institution, and whether or not those agreements purported on their face to exclude any terms other than those contained in the four corners of the signed agreement. It is unlikely, however, that a court would apply a contract which had not been subject to any significant negotiation, which was in fact a standard form contract, and which is unlikely in any event to provide a comprehensive code for all aspects of the customer bank relationship, to preclude a remedy based on the privacy code in appropriate circumstances.

An argument further runs that privacy codes have been adopted pursuant to requirements in applicable financial services legislation, such that they may be enforceable as quasi-statutory instruments and have the force of public law.

¹⁶⁹ *Georgia Construction Co. v. Pacific Great Eastern R. Co.*, [1929] 4 D.L.R. 161 at 163 (S.C.C.).

¹⁷⁰ There are a number of cases in which certain standards imposed legislatively in building codes or labour codes were held to be implied terms in contracts, but these cases are of limited use for the purposes of this discussion.

¹⁷¹ (1977) 5 A.R. 83 (S.C.).

¹⁷² [1995] B.C.J. No. 516 (B.C.S.C.), affirmed (1996), 136 D.L.R. (4th) 644 (C.A.).

Legislative Provisions Respecting Financial Institutions and Confidentiality

Federal Legislation Relating to Financial Institutions

The federal statutes that govern generally the corporate status, governance and regulation of financial institutions in Canada are the *Bank Act*,¹⁷³ the *Insurance Companies Act*,¹⁷⁴ the *Trust and Loan Companies Act*¹⁷⁵ and the *Cooperative Credit Associations Act*.¹⁷⁶ These statutes protect the personal information of customers in five different ways. First, three of the Acts allow the Governor in Council to make regulations concerning the use of customer information. Second, financial institutions are required to take reasonable precautions to ensure the protection and accuracy of their records. Third, the directors of a financial institution are required to establish procedures restricting the use of confidential information. Fourth, regulations made pursuant to the Acts place restrictions on the ability of certain institutions to share information with others. Finally, financial institutions are required to maintain certain records in Canada, although the processing of information may occur off-shore if the Office of the Superintendent of Financial Institutions grants an exemption order.

Regulation-Making Power Relating to Customer Information

Until the early 1990s, there was no provision in the federal statutes that governed financial institutions to permit the government to make regulations respecting privacy or information generally.¹⁷⁷ In 1991, the old statutes were repealed and replaced with the present statutes. The new *Bank Act*, *Insurance Companies Act*, and *Trust and Loan Companies Act* included a provision stating that: “The Governor in Council may make regulations governing the use by a company of any information supplied to the company by its customers.”¹⁷⁸ (However, the new *Cooperative Credit Associations Act* did not include a similar provision.)

In 1997, the regulation-making provision in the *Bank Act*, *Insurance Companies Act*, and *Trust and Loan Companies Act* was repealed and replaced with a provision that granted the Governor in Council a more specific ability to regulate the use of information. The new provisions in the three Acts state that the Governor in Council may make regulations:

- requiring a financial institution to establish procedures regarding the collection, retention, use and disclosure of any information about its customers or any class of customers;

¹⁷³ S.C. 1991, c. 46 as amended.

¹⁷⁴ S.C. 1991, c. 47 as amended.

¹⁷⁵ S.C. 1991, c. 45 as amended.

¹⁷⁶ S.C. 1991, c. 48 as amended.

¹⁷⁷ The existing legislation consisted of the following statutes: the *Bank Act*, R.S.C. 1985, c. B-1, *Loan Companies Act*, R.S.C. 1985, c. L-12, *Trust Companies Act*, R.S.C. 1985, c. T-20, *Canadian and British Insurance Companies Act*, R.S.C. 1985, I-12, *Foreign Insurance Companies Act*, R.S.C. 1985, I-13, and *Cooperative Credit Associations Act*, R.S.C. 1985, c. C-41.

¹⁷⁸ S.C. 1991, c. 46, s. 459; S.C. 1991, c.47, s. 489; and S.C. 1991, c.45, s. 444.

- requiring a financial institution to establish procedures for dealing with complaints made by customers about the collection, retention, use or disclosure of information about the customer;
- respecting disclosure by a financial institution of information relating to information procedures and complaint procedures;
- requiring a financial institution to designate officers and employees responsible for implementing information procedures and for receiving and dealing with customer complaints;
- requiring a financial institution to report information relating to customer complaints on information matters and the actions taken by the institution to deal with such complaints; and
- defining “information”, “collection” and “retention” for the purposes of the regulations.¹⁷⁹

In effect, this detailed provision allows the federal government to make regulations that would require a financial institution to implement a privacy code.

At the time of the writing of this study (Spring 1998) federal officials were in the process of preparing draft regulations under this provision. The draft regulations are expected to contain the following elements: Federally-regulated financial institutions will be required to establish procedures governing the collection, use and retention of customer information, and also for handling complaints relating to such matters. Institutions will be required to provide customers (perhaps *all* customers) with a written summary of their information and complaint handling procedures. There will be some form of annual reporting requirement, so that regulators may monitor the number of privacy complaints received by institutions. It is expected that the draft regulations will be released in Spring 1998, and that final regulations may be in place as soon as Summer 1998. Consultation with the industry prior to release of the draft regulations has not been entirely supportive. Proposed provisions such as requiring a mass mailing respecting privacy to all customers have been resisted on the basis that the cost of any such action is not at present warranted.

Protection and Accuracy of Records

Prior to 1991, s. 157(3) of the *Bank Act* provided that a bank and its agents shall take reasonable precautions to: “(a) prevent loss or destruction of, (b) prevent falsification of entries in, [and] (c) facilitate detection and correction of inaccuracies in the registers and records required or authorized by this Act to be prepared and maintained.” In 1991, the *Bank Act* section was

¹⁷⁹ S.C. 1991, c. 46, s. 459 as amended by 1997 c. 15, s. 55; S.C. 1991, c.47, s. 489 as amended by 1997 c. 15, s. 263; and S.C. 1991, c.45, s. 444 as amended by 1997, c. 15, s. 385. This same provision is repeated a second time in the *Insurance Companies Act* in order to give the Governor in Council the authority to make similar regulations with respect to foreign companies as well. See: S.C. 1991, c. 47 s.607 as amended by S.C. 1997, c.15, s.314.

amended to add paragraph (d), which provides that reasonable precaution shall be taken to “ensure that unauthorized persons do not have access to or use of information” in the required registers and records.¹⁸⁰ Provisions identical to the amended s. 157(3) were also included, for the first time, in the newly enacted *Insurance Companies Act*, *Trust and Loan Companies Act* and *Cooperative Credit Associations Act*.¹⁸¹ This provision remains in force in all of the Acts.

Directors’ Policies Respecting Confidential Information

Prior to 1991, there were no provisions in any of the Acts specifically requiring the directors to develop internal policies with respect to the use of confidential information. Since 1991, however, each of the federal Acts governing financial institutions stipulate that the directors of a financial institution shall “establish procedures to resolve conflicts of interest, including techniques...for restricting the use of confidential information.”¹⁸²

Restrictions on the Use of Customer Information

Two federal regulations that restrict the sharing of customer information have been enacted under the federal financial statutes. The *Insurance Business (Banks) Regulations*¹⁸³ under the *Bank Act* prohibit a bank or any one of its subsidiaries from providing any insurance company, agent or broker with any information respecting a customer or employee of the bank or the subsidiary. In effect, the regulations limit the ability of banks to share customer information with other companies or subsidiaries for insurance purposes, regardless of customer consent. The *Credit Information (Insurance Companies) Regulations*¹⁸⁴ under the *Insurance Companies Act* prohibit a company from using credit information obtained from customers in the promotion of an insurance company, agent, broker or policy unless certain qualifications are met. The regulation also prohibits a company or its subsidiary from directly or indirectly providing an insurance company, insurance agent or broker with any consumer credit information.

Storing and Processing Customer Information

Under the provisions of federal statutes, a financial institution is required to maintain, in Canada, daily records showing particulars of each customer’s transactions with the institution and the balance owing to or from each customer.¹⁸⁵ In general, the financial institution must perform all processing of data that relates to the preparation and maintenance of these customer records in Canada. However, off-shore processing of this information may occur if the Superintendent of Financial Institutions issues a special exemption order.¹⁸⁶ In such a case, the processing will be governed by the terms and conditions of the exemption order. Although these provisions may

¹⁸⁰ S.C. 1991, c. 46, s.157(3).

¹⁸¹ S.C. 1991, c. 47, s. 267; S.C. 1991, c. 45, s. 249; S.C. 1991, c. 45, s. 241, respectively.

¹⁸² S.C. 1991, c. 46, s. 157(2)(c); S.C. 1991, c.47, s. 165(2)(c); S.C. 1991, c.45, s. 161(2)(c) and S.C. 1991, c. 48, s. 167(2)(c).

¹⁸³ SOR/92-330, made under s. 416 of the *Bank Act*.

¹⁸⁴ SOR/97-11, made under s. 489 of the *Insurance Companies Act*.

¹⁸⁵ S.C. 1991, c. 46, s. 238; S.C. 1991, c. 47, s. 261; S.C. 1991, c. 45, s. 243; S.C. 1991, c. 48, s. 235.

¹⁸⁶ S.C. 1991, c. 46, s. 245(1); S.C. 1991, c. 47, s. 268(1); S.C. 1991, c. 45, s. 250(1); S.C. 1991, c. 48, s. 242(1).

protect the privacy of individuals' records, it should be noted that they have been administered principally with a view to the protection and security of data.

The Superintendent of Financial Institutions has issued guidelines outlining the circumstances under which an exemption order may be granted.¹⁸⁷ Three requirements must be met before an order is granted.¹⁸⁸ First, the Superintendent must have adequate access to the information. The laws of the jurisdiction where the data processing will occur, as well as the contracts or other legal arrangements related to it, must entitle the Superintendent to reasonable and timely access to the financial institution's information. Second, the processing of the data off-shore must not have a significant negative impact on the institution's business operations and services in Canada. This includes a consideration of whether there are adequate back-up facilities to handle operations without a major disruption of service. Third, the laws of the country in which the information is to be maintained and processed must be compatible with those of Canada. The laws of the jurisdiction where the processing will occur must not prevent a financial institution from doing anything with the information that it is reasonably expected to do in Canada. The Superintendent has also indicated that an exemption order may be subject to a time limit, any terms and conditions the Superintendent thinks fit, and the filing of any contract or procedures respecting the off-shore maintenance and processing of the information or data.¹⁸⁹

Provincial Legislation and Issues

Financial institutions may be subject to various provincial statutes which provide for the protection of information privacy in certain circumstances. These statutes fall into three main categories: statutes governing credit unions and co-operative associations, provincial Privacy Acts, and statutes governing credit reporting activities.¹⁹⁰

Several provinces have statutes that govern the actions of provincial credit unions or co-operative associations. These statutes include provisions protecting the privacy of customer information. For example, the Ontario *Credit Union and Caisses Populaires Act*¹⁹¹ requires the directors, officers, committee members and employees of a credit union to keep as confidential any information received by the credit union or any information respecting members' transactions with the credit union. The Alberta *Credit Unions Act*¹⁹² provides that regulations may be made under the Act with respect to the confidentiality of information that credit unions possess. The

¹⁸⁷ S.C. 1991, c. 46, s. 245(7); S.C. 1991, c. 47, s. 268(7); S.C. 1991, c. 45, s. 250(7); S.C. 1991, c. 48, s. 242(6).

¹⁸⁸ Office of the Superintendent of Financial Institutions Canada, *Processing Information Outside Canada*, Guideline E-3, May 1992, available at www.osfi-bsif.gc.ca.

¹⁸⁹ *Ibid.*

¹⁹⁰ In addition, there are a number of miscellaneous statutes that have some impact on privacy and personal information. In British Columbia, the *Financial Institutions Act*, R.S.B.C. 1996, c. 141, stipulates that a financial institution must not communicate information about a customer except as necessary to perform the transaction (ss. 95 and 218). The *British Columbia Insurance Licensing Regulation* also requires that any insurance agent who receives customer information shall not communicate the information except as necessary to perform his or her duty. In Alberta, the *Financial Consumers Act*, S.A. 1990, c. F.9.5, imposes restrictions on a supplier, agent or financial planner with respect to their use of personal finance information provided by a consumer (s. 18).

¹⁹¹ S.O. 1994, c.11, s. 143.

¹⁹² S.A. 1989, c.31.1, s. 226.

Saskatchewan *Credit Union Act*¹⁹³ stipulates that registers of members of a credit union are to be kept confidential and cannot be released without the authorization of the board. Legislation in both New Brunswick and Newfoundland impose a duty on credit unions to take reasonable precautions to ensure the protection and accuracy of records.¹⁹⁴ In addition, British Columbia and Newfoundland each have Acts that specifically govern cooperative associations.¹⁹⁵ In these Acts, cooperative associations are required to maintain the confidentiality of all member information unless the member otherwise consents to the information's release.

Four common law jurisdictions in Canada have recognized a right to privacy in tort through statute. Statutes in Newfoundland,¹⁹⁶ Saskatchewan,¹⁹⁷ Manitoba,¹⁹⁸ and British Columbia¹⁹⁹ establish tort liability for invading the privacy of another person and permit actions to be brought without proof of damage. None of these statutes define the term "privacy"; thus, interpretation of what constitutes an invasion of privacy is left to the courts. To date there has been relatively little judicial consideration of these statutory provisions.²⁰⁰ In general, courts considering actions under these provincial statutes have looked to the facts in each case to determine whether there was an unreasonable violation of privacy. As noted above in the discussion of the common law tort of invasion of privacy, it is possible that the statutory privacy tort would apply to the collection and use of personal information. However, cases decided under the privacy statutes have involved situations with an element of physical intrusion; as a result, it remains unclear whether the statutory tort is broad enough to apply to information.

Finally, most provinces have enacted consumer reporting legislation which attempts to balance the value of protecting informational privacy with the value of extending credit to worthy individuals.²⁰¹ Consumer reporting agencies (also known as credit bureaux) collect information about individuals and sell it to other interested businesses, such as financial institutions, which use the credit reports to determine whether or not they will extend credit to a customer.²⁰² The reports produced by such agencies must be fair and accurate, as inaccurate information may lead

¹⁹³ S.S. 1984-85-86, c. 45.1, s. 27.

¹⁹⁴ *Credit Unions Act*, S.N.B. 1992, c. C.32.2, s. 28; *Credit Unions Act*, S.N. 1997, c. C.37.1, s.28.

¹⁹⁵ *Cooperative Association Act*, R.S.B.C. 1996, c. 71, s. 47; *Cooperative Societies Act*, R.S.N. 1990, c. C-35, s.24.

¹⁹⁶ *Privacy Act*, S.N. 1981, c. 6.

¹⁹⁷ *Privacy Act*, R.S.S. 1978, c. P-24.

¹⁹⁸ *Privacy Act*, R.S.M. 1987, c. P-125.

¹⁹⁹ *Privacy Act*, R.S.B.C. 1979, c. 336.

²⁰⁰ For some discussion of the case law decided under these statutes, see: Lawson, *supra*, note 116 at 87-95.

²⁰¹ *British Columbia Credit Reporting Act*, R.S.B.C. 1996, c.81; *Manitoba Personal Investigations Act*, R.S.M. 1987, c. P.34 as amended; *Newfoundland Consumer Reporting Agencies Act*, R.S.N. 1990, c. C-32, as amended; *Nova Scotia Consumer Reporting Act*, R.S.N.S. 1989, c. C.93; *Ontario Consumer Reporting Act*, R.S.O. 1990, c. C-33 as amended; *Prince Edward Island Consumer Reporting Act*, R.S.P.E.I. 1988, c. C-20 as amended; *Saskatchewan Credit Reporting Agencies Act*, R.S.S. 1978, c. C-44, as amended; Quebec's *An Act respecting the Protection of Personal Information in the Private Sector*, S.Q. 1993, c. P.39.1, as amended. Alberta, and New Brunswick do not have legislation governing consumer credit reporting agencies.

²⁰² For some general discussion of credit reporting, see: Dale Gibson, "Regulating the Personal Information Industry," in *Aspects of Privacy Law: Essays in Honour of John M. Sharp*, ed. by Dale Gibson (Toronto, Butterworths, 1980) 111 at 113.

to unfair denials of credit and other benefits.²⁰³ Consumer reporting statutes limit the sort of information that may be reported and establish rights of access to the individual's own information, so that the individual may check the accuracy of his or her records. In addition to these statutes, some credit bureaux have adopted their own privacy codes or guidelines. For example, Equifax Canada Inc., a leading credit bureau company, has adopted a code of conduct for its information handling practices.²⁰⁴

While consumer reporting statutes specifically govern the business of consumer credit reporting agencies, they also contain provisions to which financial institutions must adhere. For example, financial institutions generally may obtain customer information from a credit reporting agency only upon written consent of the consumer²⁰⁵ or upon notice to the consumer.²⁰⁶ In some provinces, financial institutions also must inform a consumer, at the consumer's request, whether a consumer report has been referred to in connection with a transaction and, if so, must provide the consumer with the name and address of the consumer reporting agency supplying the report.²⁰⁷ The statutes generally stipulate that when a benefit is refused on the basis of a consumer credit report, the consumer is entitled to know the name and address of the agency and the source of information on which the negative decision was based.²⁰⁸ As well, in Ontario, a financial institution extending credit to a consumer cannot supply a list of names and criteria to a credit reporting agency in order for the agency to determine which names meet the criteria without first notifying the consumer in writing of its intention to do so.²⁰⁹

One of the biggest concerns relating to privacy in the financial services sector is raised by the credit bureau. The credit bureau is an institution with no direct dealings or relationship with consumers, largely unknown and misunderstood, maintaining large databases of information which may or may not be accurate.²¹⁰ It has the power to determine whether or not an individual is given credit to consolidate his or her bills, buy a home or start a business; it is the epitome of the remote database, in its size and potential for harm equalled only by the comprehensive records of taxation authorities. Justifiably, the ability to use and share information with credit bureaux is regulated. However, not all provincial regulation is up to the same standard. Requirements that individuals be informed of the use of a credit bureau, of the location and the

²⁰³ However, at least one study suggests that errors are relatively common in agency records. In 1991, *Consumer Reports* reported that a study of 1,500 files held by the three largest U.S. reporting agencies found errors in 43 per cent of all the files, although the industry disputed the findings. The magazine's own staff requested 30 summaries of their files from the three national reporting companies and found them "hard to decipher, incomplete and sometimes inaccurate." See: "What Price Privacy?" *Consumer Reports* (May 1991) 356.

²⁰⁴ For a brief discussion of the privacy measures taken by Equifax Canada Inc., see that company's Web site at www.equifax.ca.

²⁰⁵ R.S.P.E.I. 1988, c. C-20, s. 10; R.S.O. 1990, c. C-33, s. 8; R.S.B.C. 1996, c.81, s. 12; R.S.M. 1987, c. P.34, s. 3; R.S.N. 1990, c. C-32, s. 19; R.S.N.S. 1989, c. C.93, s. 11.

²⁰⁶ R.S.P.E.I. 1988, c. C-20, s. 10. R.S.O. 1990, c. C-33, s. 10, R.S.B.C. 1996, c.81, s. 12; R.S.M. 1987, c. P.34, s. 3; R.S.N. 1990, c. C-32, s. 23; R.S.N.S. 1989, c. C.93, s. 11.

²⁰⁷ R.S.S. 1978, c. C-44, as amended s.21, R.S.O. 1990, c. C-33, s. 10; R.S.P.E.I. 1988, c. C-20, s. 10. R.S.N. 1990, c. C-32, s. 22; S.Q. 1993, c. P.39.1, s. 19.

²⁰⁸ R.S.B.C. 1996, c.81, s. 13; R.S.M. 1987, c. P.34, s. 6; R.S.N.S. 1989, c. C.93, s. 11; R.S.O. 1990, c. C-33, s. 10; R.S.P.E.I. 1988, c. C-20, s. 10.

²⁰⁹ R.S.O. 1990, c. C-33, s. 11.

²¹⁰ *Consumer Reports*, *supra*, note 203.

contact person for the credit bureau, and of the right to see any credit bureau report would appear to be fundamental. As the federal government has no authority to legislate in this area, the provinces should be encouraged to review their legislation to ensure it meets certain uniform standards. We have not conducted the same investigations of complaints and voluntary practices in the credit reporting sector; thus, while theoretical concerns arise, we cannot judge to what extent they are met by present practice.

A further concern related to provincial jurisdiction is the sharing among insurers of health information. The regulation of insurance is a matter of provincial jurisdiction, based on the provinces' constitutional power to regulate property and civil rights.²¹¹ Historically, the right to incorporate and to regulate insurance companies has been acquired by the federal government and largely acceded to by the provinces. However, there appears to be no constitutional basis for such federal jurisdiction, as there is with the exclusive federal jurisdiction over banking. In any event, the regulation of the conduct of insurance transactions and relationships between insurers and their customers is clearly within the provincial jurisdiction.

Insurers routinely share health information through the Medical Information Bureau, Inc. (MIB), an information clearinghouse with its main office near Boston, Massachusetts.²¹² Established by the insurance industry, the MIB is intended to prevent fraud by serving as a central repository of medical facts about insured persons. About 680 member insurers in Canada and the United States provide basic information about insured persons to the MIB, based on an authorization included in the insurance application form. The MIB makes this information available to its member insurance companies, on request, in coded reports. The report consists of the person's name, birth date, birth state, occupation and general area of residence, together with a string of codes representing medical conditions and certain non-medical attributes.²¹³ The MIB report is intended to function as an alert only; an insurer who requests a report is required to conduct an underwriting investigation rather than rely on the report alone to make a decision about an insurance applicant. The MIB does not provide information to non-members, except under the terms of a court order, and MIB members are required by the terms of their agreements with the MIB to keep reports confidential. Canadian residents may apply to the MIB at its Toronto office to gain access to their reports; individuals also may request corrections of inaccurate information.

²¹¹ See: Peter W. Hogg, *Constitutional Law of Canada*, Looseleaf edition, volume 1 (Scarborough, Ont.: Carswell, updated to 1997) at p. 24-7: "[T]he insurance industry was the battleground upon which federal and provincial regulators fought for control in a series of cases between 1880 and 1942. These cases were all resolved in favour of the provincial power over property and civil rights. Insurance companies are therefore subject to provincial regulation, although there is also a considerable federal presence which seems to be based as much on acquiescence by the provinces and the industry as on constitutional right."

²¹² For further information about the MIB, see: *Medical Information Bureau: A Consumer's Guide* (undated), published by the MIB, and Consumers' Association of Canada, *Privacy and Data Protection: Background Paper* (Consumers' Association of Canada, July 1992) at 68-70.

²¹³ There are about 210 medical codes: "Conditions most commonly reported include height and weight, blood pressure, EKG readings and x-rays if, and only if, these facts are commonly considered significant to health or longevity." There are five codes representing non-medical information, including an adverse driving record, participation in hazardous sports and aviation activity. See: *Medical Information Bureau: A Consumer's Guide*, *supra*, note 212 at 6.

To our knowledge, there is no Canadian legislation that regulates the operation of the MIB or guarantees the access and correction rights of Canadian residents.²¹⁴ While the MIB performs a useful function, its operations may raise legitimate privacy concerns. There is a strong argument that to the extent an insured's health information is shared through the MIB in the same manner that financial information is shared through credit bureaux, the MIB – or the insurers who use the MIB's services – should be subject to similar provincial regulation. On the other hand, the limited nature of the information in the MIB report and the fact that MIB members are required to conduct an independent investigation after receiving a report somewhat mitigate privacy concerns. Further investigation of the MIB and the manner in which Canadian insurers use the MIB's services would be appropriate to determine whether regulation is needed. Some provinces are considering medical information statutes; in particular, the proposed Ontario statute might apply to an insurers' disclosure of information to the MIB or use of information received from the MIB.²¹⁵ As the regulation of the activities of insurers is a matter of provincial jurisdiction, provincial officials might be encouraged to further study the issue of the sharing of health information.

Quebec's Private Sector Privacy Legislation

The only province with statutory provisions that regulate the collection, use, transfer and retention of personal information throughout the private sector is Quebec. Quebec's *Act respecting the protection of personal information in the private sector* (also known as Bill 68) expands and clarifies certain privacy rights first set out in the province's new *Civil Code*.²¹⁶ The Act came into force on January 1, 1994²¹⁷ and applies to a wide range of private sector entities, including corporations, sole proprietorships, partnerships, organizations and associations.²¹⁸ It represents the first legislation in North America imposing privacy principles on the private sector as a whole, and has important implications for Canada. As Professor Colin J. Bennett wrote: "At the moment, Canada is the only country in which the scope of privacy protection in one of its member jurisdictions exceeds that of the federal government."²¹⁹

On a literal reading, the Act applies to banks as well as other financial institutions. However, it is an open question whether the provincial Act may apply to banks, as banking is a head of jurisdiction assigned to the federal government by the *Constitution Act*, 1867.²²⁰ In a 1994 article, lawyer Etienne DuBreuil acknowledged that banks might challenge the application of the

²¹⁴ However, state privacy legislation in Massachusetts may apply to the operations of the MIB. See: Consumers' Association of Canada, *Privacy and Data Protection: Background Paper*, *supra*, note 212 at 69.

²¹⁵ See Part I of this study, footnotes 64 to 67 and accompanying text.

²¹⁶ R.S.Q. c. P-39.1. The Act expands and clarifies certain rights of privacy and access to information set out in articles 35 to 41 of the *Civil Code of Quebec*.

²¹⁷ Note, however, that certain provisions did not come into force until six months or one year after January 1, 1994. See the original enactment of the Act: S.Q. 1993, c. 17, ss. 114 and 115.

²¹⁸ The definitions of the entities covered by the Act may be found in ss. 1, 96 and 97 of the Act and article 1525 of the *Civil Code of Quebec*.

²¹⁹ Colin J. Bennett, *Implementing Privacy Codes of Practice*, PLUS 8830 (Etobicoke, Ont.: Canadian Standards Association, 1995) at 10.

²²⁰ R.S.C. 1985, Appendix II, No. 5.

Act as unconstitutional but argued that there was a good chance that the Act's application would be upheld.²²¹ He noted that, in the absence of federal legislation on a particular subject matter, validly enacted provincial law may apply to a federal undertaking unless the law prevents the federal undertaking from managing its operations or generally accomplishing its ends. Assessing the Quebec privacy legislation, DuBreuil wrote:

In the context at hand, we can draw a first conclusion to the effect that the Federal Parliament has not enacted legislation dealing with the protection of personal information in the private sector. That being the case, it is our view that this legislation is applicable to Federal enterprises. Bill 68 will therefore be applicable to all enterprises carrying on their activities in the province of Quebec. Perhaps the only challenge to this application of Bill 68 would be a judicial ruling to the effect that the Federal enterprise is being paralysed in carrying on its business or managing its operations. To paraphrase the jurisprudence, the court would have to be satisfied that the Provincial law is preventing the Federal legislation from accomplishing the very object for which it is created.²²²

While the present study does not purport to assess the constitutionality of the application of Bill 68, the authors note it is possible that proposed regulations requiring banks to adopt privacy codes would affect DeBreuil's analysis. Arguably, the federal regulations might be seen as precluding the application of provincial privacy legislation.

The Quebec Act contains a variety of provisions that govern the collection of "personal information," which it defines as information that relates to an individual and that allows the individual to be identified.²²³ For example, a business must assign an object to a file of personal information on the establishment of the file; moreover, if the business collects information directly from the individual, it must inform the individual of the existence of the file. A business may collect only information which is necessary to the object of the file.²²⁴ As well, a business must collect information directly from the individual, subject to certain exceptions, and must collect information only by lawful means.

²²¹ Etienne DuBreuil, "Quebec Bill 68: Is it Sufficient for the Federal Canadian Financial Institutions Sector?" in *Privacy in Financial Services: Striking a Balance between Privacy Rights and Profits* (Toronto: Canadian Institute, April 27, 1994).

²²² *Ibid.*, at 6-7. Note, however, that DuBreuil also cautions that his article not be read as a legal opinion on the constitutionality of Bill 68. Later, Professor Colin J. Bennett noted that while the jurisdictional issues relating to Bill 68 remained unresolved, entities within the federally-regulated private sector such as banks and airlines had declared their willingness to abide by the legislation. See: Bennett, *supra*, note 219 at 10.

²²³ R.S.Q. c. P-39.1, ss. 1, 2 and 4 to 9. Note that s. 1 states that the Act does not apply to journalistic material which is collected or used for the purpose of informing the public.

²²⁴ While the Act states that a business may collect only information "necessary" to the object of the file, the Civil Code states that a business may collect only information "relevant" to the object of the file. See: R.S.Q. c. P-39.1, s. 5, and *Civil Code of Quebec*, article 37.

Other provisions apply to the use and transfer of personal information.²²⁵ Businesses must ensure that personal information is up-to-date and accurate when it is used to make a decision affecting the individual. In general, businesses are prohibited from disclosing, transferring or using personal information for purposes that are “not relevant” to the object of the individual’s file. Other uses, disclosures or transfers are permitted only where the individual consents to them or one of the exceptions set out in the Act applies.²²⁶ The Act provides a narrow definition of individual consent: “Consent to the communication or use of personal information must be manifest, free and enlightened, and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purposes for which it was requested.”²²⁷ The Act also prohibits a business within Quebec from making an extra-provincial transfer unless the transferor has taken “all reasonable steps” to satisfy itself that the information will be protected in the new jurisdiction.²²⁸

Special provisions apply to “nominative lists,” which are defined as lists of individuals’ names, addresses and phone numbers.²²⁹ The Act states that when a business seeks to use its own nominative list for commercial or philanthropic canvassing, the individuals named on the list must be given a valid opportunity to request that their names be deleted. When a business seeks to transfer its own nominative list to another business, it must ensure that the list will be used only for commercial or philanthropic canvassing and, before transfer, ensure that the individuals named on the list have a valid opportunity to have their names deleted. In either case, the provincial agency responsible for the Act takes the position that the business must send a letter to each individual named on the list with instructions on how to have his or her name deleted.²³⁰ Finally, a person who solicits by telephone or mail on the basis of a list must inform the individual being contacted of the right to have his or her name deleted from the list.

The Act also fleshes out rights of access to and correction of personal information which are set out in the *Civil Code of Quebec*.²³¹ Under the Act, the business must confirm the existence of a file of personal information on the individual’s request and answer an access request within 30 days of its receipt. The business must provide access free of charge, except for a reasonable fee that may be charged for the transcription, reproduction or transmission of information. In addition to the Civil Code’s rights of correction, the individual can require the business to delete

²²⁵ R.S.Q. c. P-39.1, ss. 10 to 26.

²²⁶ There are more than a dozen exceptions set out in the Act. See: R.S.Q. c. P-39.1, ss. 18 and 21.

²²⁷ R.S.Q., c. P-39, s. 14.

²²⁸ *Ibid.*, s. 17.

²²⁹ *Ibid.*, ss. 22 to 26.

²³⁰ Commission d’accès à l’information du Québec, *Contact / Advice on the Confidentiality of Personal Information: Direct Marketing* (January 1995).

²³¹ See: *Civil Code of Quebec*, articles 37-40, and R.S.Q. c. P-39.1, ss. 27 to 41.

information in his or her file which was collected “otherwise than according to law.” However, the Act also sets out exemptions and limits to the access right.²³²

The Quebec Act should have a significant effect on the collection and use of all types of personal information by financial institutions. A financial institution which intends to collect information must reveal this fact to the individual and establish a file on the individual with a stated object. Information collected must be used only for purposes relevant to the object of the file, unless one of the exceptions in the Act applies. The institution must establish methods by which customers may have access to their information. If the institution intends to use information for the assembly of lists to be used for commercial or philanthropic soliciting, it will face the application of the Act's onerous provisions relating to nominative lists. Thus, for example, an institution would be unable to compile a list of customer's names for sale to other businesses without giving those customers a valid opportunity to have their names removed from the list. Moreover, the effects of the Quebec Act will not be confined to the province. National institutions will face the Act's restriction on the extra-provincial transfer of information. As a practical consequence, they may be required to avoid extra-provincial transfers of personal information about Quebec residents or adopt measures similar to those required by the Act at offices across Canada.

Industry Association Codes

The period since the early 1980s has seen a proliferation of corporate codes intended to protect the privacy interests of customers of financial institutions.²³³ In the 1980s and 1990s, industry associations for banks, insurers and trust companies adopted model codes for use by their members.²³⁴ Responding to pressure from government and industry associations, many financial institutions have adopted codes based on their association model codes. While these privacy codes do not have the force of law, they represent a significant commitment to privacy principles. A customer with concerns about the collection or use of personal information may launch a privacy complaint or apply for access to the information under the institution's privacy code. The main industry model codes are discussed below.

²³² The Act places a limit on the access right of some minors, stating that there is no right for a person less than 14 years of age to gain access to information of a medical or social nature. The Act also establishes a small set of exemptions to the access right. The main mandatory exemption requires the business to withhold personal information about an individual other than the requester if disclosure might seriously harm that individual. Three permissive exemptions permit disclosure to be withheld of: (1) health information where disclosure would result in serious harm to the individual's health; (2) information that would likely hinder investigations of a security service, security agency, or a detective agency; and (3) information that would likely affect judicial proceedings in which either the business or the individual has an interest.

²³³ For discussion of privacy codes and financial institutions, see: Richard C. Owens, Tom Onyshko, and Peter C. Goode, “Reform Proposals Relating to Customer Privacy and Tied Selling in the Federally-Regulated Financial Services Sector” in *The Regulation of Financial Institutions: Issues and Perspectives* (Scarborough: Carswell, 1997) 143 at 153ff.

²³⁴ In the 1990s, federal statutes governing financial institutions banks, insurers and trust companies were amended to require such institutions to adopt procedures restricting the use of confidential information. More recently, the federal statutes governing banks, trust and loan companies and insurance companies were amended to permit the government to issue regulations requiring privacy codes. For further discussion see this Part under the heading Legislative Provisions Respecting Institutions and Confidentiality.

It should be noted that attempts were made to obtain information about the privacy codes, if any, of the Investment Dealers Association of Canada and three particular investment dealers, which were unsuccessful.²³⁵

Canadian Bankers Association

The Canadian Bankers Association (CBA) adopted a *Model Privacy Code for Individual Customers* in 1990 after consultations with the federal government, provincial governments and the Consumers Association of Canada.²³⁶ The code relied substantially on the principles set out in the OECD guidelines.²³⁷ It set out principles relating to the collection of personal information, the quality of personal information, specifying the purposes of personal information, limiting the use of personal information, security safeguards, individual participation, accountability and openness.

Various provisions in the code related to the collection stage. For example, banks were directed to obtain information "primarily" from customers themselves, but permitted to consult external sources such as credit grantors, credit bureaux, income sources and personal references. Under section 5(a), banks were permitted to collect personal information for a variety of purposes: "establishing and maintaining relationships with customers; offering and providing products and services as permitted by law; complying with the law; and protecting customers' and banks' interests." Banks also were required to advise customers at the time of collecting information of the use of that information, and to obtain consent to obtain further information from external sources.

Other provisions related to the use of information. Where personal information was used for purposes other than those for which it was collected (or a compatible purpose) the bank was required to obtain the customer's consent. Banks were permitted to release information to third parties only for four purposes, which were based on the four *Tournier* categories: in the case of the customer's consent, in order to fulfil a legal obligation, to protect the bank's interests, and in the case where there is a significant public interest requiring disclosure. However, the definition of the bank's own interest was very vague, offering as an example that "various court proceedings may require that personal information on customers' accounts be introduced as evidence."²³⁸ Banks were required to keep information only for the purposes set out in section 5(a) and to

²³⁵ The Investment Dealers Association of Canada did not provide any materials to the authors and indicated that it did not wish to participate in the author's study. An articling student assigned to obtain the privacy codes of three large investment dealers was unable to do so. In one case, he was told that no such information was available. In the two other cases, his calls were not returned by representatives of the investment dealers.

²³⁶ Canadian Bankers Association, *Model Privacy Code for Individual Customers* (1990). It is worth noting that the CBA submitted a model code of privacy principles to its membership in 1986, but this earlier attempt at a code was rejected by the membership. See Bennett, *supra*, note 219 at 26. For further discussion of the 1990 CBA code, see Edward K. Rowan-Legg, "Confidential Information" in *I've Got A Secret: The Duty of Confidentiality in the Private Sector* (Toronto: Canadian Bar Association - Ontario, March 1994).

²³⁷ For discussion of the OECD guidelines, see Part I of this study under the heading The Nature of Privacy and Informational Privacy Issues: Computerization and Personal Information Principles.

²³⁸ CBA, 1990 model code, *supra*, note 236, s. 6(c).

ensure that information remained as accurate as possible and as complete as required for the purpose.

The customer's right of access was also set out in the code.²³⁹ However, the access right extended only to factual information about the individual and not "to opinions or judgments about them" which were held by the bank. The code permitted banks to take a reasonable time and charge a reasonable fee for access. If access was refused, the bank was required to provide reasons for the refusal. Customers who received access had a right to challenge the accuracy of personal information; any differences about the accuracy of information were to be "noted". The bank had a duty to pass on corrections to third parties only where the inaccuracy might result in a customer's interests being harmed. Banks were required to maintain a list of disclosures of information along with the customer records, except for routine disclosures which did not have to be noted.

Other provisions in the code required security safeguards to protect the privacy of personal information, stated that banks were to delegate a senior officer responsible for privacy protection, and stated that privacy policies (including complaint procedures) were to be made known to customers. If customers were unhappy with the way a complaint was handled, they could contact the Office of the Superintendent of Financial Institutions.

The 1990 CBA code was criticized by the federal Privacy Commissioner and the Consumers' Association of Canada.²⁴⁰ The Privacy Commissioner pointed to the code's limitation on the individual's access rights and its vaguely defined exceptions permitting disclosure. For example, Commissioner Phillips wrote in 1994:

The Canadian Bankers Association code (and those of the individual banks) does not cover subjective information about individual clients nor do they protect bank employees. Broad disclosures are allowed to serve the banks' business interest (as anyone who has read the fine print at the bottom of a bank card application will attest). And the codes will do nothing to prevent banks exchanging clients' personal information with the insurance companies and stock brokerages they may now own following recent changes to financial legislation.²⁴¹

In 1996, the CBA issued a revised version of the code – known as *Model Privacy Code: Protecting individual bank customers' personal information* – which was based on the principles of the CSA model code.²⁴² The new CBA code is more detailed, with a new emphasis on the need to obtain a customer's consent, some specific discussion of the bank's target marketing practices and a strengthening of the customer's access right. The new code consists of 10 principles: accountability; identifying the purposes of personal information; obtaining customer consent; limiting the collection of personal information; limiting the use, disclosure and

²³⁹ *Ibid.*, s. 8.

²⁴⁰ Bennett, *supra*, note 219 at 26.

²⁴¹ *Privacy Commissioner of Canada, Annual Report 1993-94* (Ottawa: Canada Communications Group, 1994) at 6. See also *Privacy Commissioner of Canada, Annual Report 1990-91* (Ottawa: Supply and Services Canada, 1991) at 16.

²⁴² For discussion of the CSA model code, see Part I under the heading Privacy Developments Relating to the Financial Services Sector in Canada, at footnotes 53 to 55 and accompanying text.

retention of personal information; keeping personal information accurate; safeguarding personal information; making information about privacy policies available; customer access to personal information; and handling complaints. The accounting firm of Price Waterhouse has provided a report confirming that the new code complies with the CSA model code.²⁴³

In the case of collection, the code sets out a new (and longer) list of purposes for which a bank may collect information: “to understand the customer's needs; to determine the suitability of the products and services for the customer or the eligibility of the customer for products and services; to set up and manage products and services that meet the customer's needs; to offer products and services that meet those needs; to provide ongoing service; to meet legal and regulatory requirements.”²⁴⁴ At the time of collection, the bank now must make the customer aware of why the personal information is needed, how the information may be used with consent for other purposes and the fact that the customer may refuse consent for other purposes. However, the new code maintains the previous approach to the source of personal information, stating that banks should collect it “primarily” from the individual but may also collect it from an external source such as credit bureaux, employers and other lenders.

In the case of consent, the code places an obligation on banks to make a “reasonable effort” to ensure that customers understand how personal information will be used and disclosed. The bank has a responsibility to obtain consent for the use and disclosure of information at the time it is collected.²⁴⁵ This consent can be express or implied, although express consent will be the “preferred” form (unlike Quebec's Bill 68, which sets strict requirements for consent to be “manifest, free, and enlightened, and [given] for specific purposes.”²⁴⁶). Implied consent will occur when a customer uses a bank product or service, or fails to respond to the bank's offer to have their personal information removed from a direct marketing list. A bank may use information without consent to detect fraud, collect overdue accounts, comply with the law, or provide information to agents of the bank who need it for banking functions (such as printing cheques). The customer may later withdraw his or her consent, subject to legal or contractual restrictions. But a withdrawal may mean that the bank is no longer able to offer certain types of products or services.²⁴⁷ For example, a bank may refuse to lend money if the customer refuses to consent to the bank obtaining a report from a credit bureau.

²⁴³ The short Price Waterhouse report is contained in the version of the CBA code issued by the Canadian Bankers Association in November 1996.

²⁴⁴ Canadian Bankers Association, *Privacy Model Code: Protecting individual bank customers' privacy* (1996), s. 2.2.

²⁴⁵ *Ibid.*, Principle 3.

²⁴⁶ See: *An Act respecting the protection of personal information in the private sector*, R.S.Q. c. P-39.1, s. 14.

²⁴⁷ This withdrawal of consent provision states in part: “Subject to legal and contractual restrictions, customers can refuse or withdraw consent at any time as long as: the bank is given reasonable notice of the withdrawal [and] consent does not relate to a credit product where the bank must report information after credit has been granted. This is to maintain the integrity of the credit system. ... Refusing or withdrawing consent for the bank to collect, use or disclose personal information could mean that the bank cannot provide the customer with some product, service or information of value to the customer.” The withdrawal of consent provision is based on a similar provision which appears in the CSA model code. See CBA 1996 model code, *supra*, note 244, s. 3.5.

Other provisions require consent before using personal information for target marketing.²⁴⁸ If a bank wishes to use personal information to market new services or products through the bank or an affiliate or subsidiary, the bank must obtain the customer's consent at the time of collection. At the time that the customer applies for a product or service and provides personal information, the bank must: "tell the customer that this personal information may be used by the bank or its subsidiaries or affiliates to market other products and services to the customer; describe the types of subsidiaries and affiliates who might market their products or services; ask the customer for consent, telling them that this use of personal information is optional."²⁴⁹

A complementary duty is imposed on subsidiaries or affiliates who offer services to bank customers. The first time that a subsidiary or affiliate discusses a product or service with the customer, the subsidiary or affiliate will explain the use to be made of the customer's personal information and give the customer an opportunity to withdraw consent for further use of information.

In the case of use and disclosure of information, the new code sets out the principle that a bank must use personal information only for the reasons for which it was collected unless the customer has consented to a new use. But the new code is less specific about the bank's ability to disclose information without consent. It states that "[u]nder certain exceptional circumstances, banks have a common law duty or right to disclose personal information to protect the bank's or public's interest without customer consent."²⁵⁰ And it states that a bank may release information to comply with the law, such as in response to subpoenas, search warrants, other court orders and demands from parties with a legal right to information. When a bank discloses to comply with the law, it should protect the customer's interests by: ensuring that the order appears to comply with the law under which it was issued; disclosing only the information that is legally required; and refusing to comply with casual requests for information from government or police.

Special provisions are included for health information. These provisions appear to be aimed at alleviating concerns that a bank will use health information for reasons other than those stated at the time of collection.²⁵¹ The code states that a bank may collect health records only for a specific purpose and that it will not disclose such records to its subsidiaries or affiliates, nor vice versa. Thus, a bank cannot use its subsidiary's records of the health of its customers to assess a loan application.

In the case of access and correction, the new code sets out in more detail the customer's right of access to personal information. One important change is that the access right is no longer limited merely to factual information; a second is that the code now sets out some of the reasons for refusal of access. Section 9.3 fleshes out the access right by stating:

²⁴⁸ *Ibid.*, s. 5.3.

²⁴⁹ *Ibid.*, s. 5.3.

²⁵⁰ *Ibid.*, Principle 5.

²⁵¹ *Ibid.*, s. 5.4. For an expression of concern about the use of health information, see Consumers' Association of Canada, *Reform of Financial Services: Retailing of Insurance by Deposit-Taking Institutions*, A submission to the federal Department of Finance (August 1995) at 16ff.

Each bank will identify who it collected the personal information from, who it has disclosed the personal information to, and how and when the information was disclosed. The bank will take this information from its records, and will provide it to the customer in a form that is easy to understand, providing explanations for abbreviations and codes. Each bank will provide the personal information to the customer within a reasonable time, and for a reasonable cost.

The code states that banks may deny access to personal information only for specific reasons which it must set out in their policies. These reasons may include the fact that the information: “may be too costly to retrieve; may contain references to other persons; may be subject to solicitor-client or litigation privilege; may contain the bank’s own ‘proprietary information’; and cannot be disclosed for legal reasons.”²⁵²

Canada’s main banks all adopted privacy codes or policies after the CBA adopted its first model code in 1990. More recently, banks have begun to revise their codes or policies to comply with the new version of the CBA model code. Various bank publications on privacy codes or policies are available to the public on request: see, for example, the Canadian Imperial Bank of Commerce’s *CIBC: Privacy Standards*; the Bank of Nova Scotia’s *Scotiabank & You: A Question of Privacy*²⁵³; the Toronto Dominion Bank’s *Protecting Your Privacy: TD’s Privacy Code*; Royal Bank’s *Straight Talk about client privacy*; the Bank of Montreal’s *Your Privacy*, and the National Bank of Canada’s *Privacy Code for Individual Customers*. (In addition, foreign banks operating in Canada such as Amex Bank of Canada, Citibank Canada, Hongkong Bank of Canada and ING Bank of Canada have published privacy materials.²⁵⁴) In general, these publications describe in broad outline the principles from the revised CBA code. However, it should be noted that an articling student assigned the task of gathering the privacy codes of banks was unable to obtain privacy codes from two smaller banks. Representatives of these banks contacted by the student were unable to provide a copy of the bank’s code or privacy materials. It should be noted that many smaller banks (but not those contacted by us) have no significant participation in the consumer market for financial services; thus, it may not be appropriate for such smaller banks to have the same framework of privacy protection.

²⁵² CBA 1996 model code, *supra*, note 244, s. 9.4. Explaining the term “proprietary information” the code states: “For example, a bank may use a scoring formula or make a collection recommendation that is confidential to the bank.”

²⁵³ The full Bank of Nova Scotia’s Privacy Code is available on the bank’s web site at <http://www.scotiabank.ca/privcode.html>.

²⁵⁴ See Amex Bank’s *American Express Privacy Code*, Citibank’s *Citibank Canada: Your Privacy*, Hongkong Bank of Canada’s *Strictly Between Us: Protecting your privacy and resolving your complaints*, and ING Bank of Canada’s *ING DIRECT: Personal Account Terms*. See also Bennett, *supra*, note 219 at 26.

Trust Companies Association of Canada

In 1993, the Trust Companies Association of Canada (TCAC) adopted a model privacy code. The TCAC's *Customer Privacy: A Matter of Trust* describes a code which is similar in its outline and most of its details to the 1990 Code of the CBA. The TCAC code sets out eight principles relating to: the collection of personal information, the quality of personal information, the purpose for collecting personal information, the use of personal information, security safeguards, the customer's right of access to and correction of personal information and dispute resolution measures. Like the first CBA code, the TCAC code limits the individual's right of access to factual information. Complaints are to be resolved by procedures established by individual trust companies.

It appears that trust companies have adopted privacy policies of their own or use the privacy codes of their parent banks. Canada Trust has its own privacy brochure – *Protecting Your Privacy* – and its own privacy policy based on the CSA model code principles, while National Trust and Montreal Trust use the privacy brochure and code of their parent bank.²⁵⁵ However, an articling student assigned the task gathering privacy codes from several other trust companies was unable to do so; these trust companies did not return phone calls or failed to provide privacy materials.

Insurance Industry Associations

Two separate associations exist for the insurance industry: the Canadian Life and Health Insurance Association (CLHIA), which represents life and health insurance companies, and the Insurance Bureau of Canada (IBC), which represents automobile and casualty insurance companies.²⁵⁶ Both associations have been active in the development of model privacy codes.

The efforts of the CLHIA predated the official publication of the OECD principles. In 1980, the association adopted a set of guidelines for its member insurers based on the draft version of OECD personal information guidelines. Professor Colin J. Bennett has noted that a variety of factors help to explain the association's early interest in privacy issues, including the fact that U.S.-based insurers had developed privacy codes in the 1970s, and the fact that provincial insurance regulators expressed some early interest in the privacy issue.²⁵⁷ Later, the association adopted a set of specific guidelines on the use of HIV information.²⁵⁸

The CLHIA moved to revise its privacy guidelines in the early 1990s, resulting in a new *Right to Privacy Guideline* published in 1993. The current version of the guidelines sets out principles

²⁵⁵ The Canada Trust privacy code is titled *Protecting Your Privacy*. (November 1997). The discussion of the approach taken by National Trust and Montreal Trust is based on interviews by N. Djordjevic with officials of National Trust and Montreal Trust in February 1998.

²⁵⁶ See Bennett, *supra*, note 219 at 28. Note that the Insurance Bureau of Canada has recently become part of another group known as the Insurance Council of Canada.

²⁵⁷ *Ibid.*, at 29.

²⁵⁸ Canadian Life and Health Association, *Guidelines with Respect to AIDS, for the Sale and Underwriting of Life and Health Insurance* (1987).

relating to the collection of personal information, the quality of personal information, specifying the purpose for personal information, the use and disclosure of personal information, individual access to personal information, complaint resolution measures, and security safeguards. The wording and general approach of the guidelines remain based on the OECD information principles. There is no provision for independent oversight; complaints are to be resolved by individual companies' own procedures. The guidelines are accompanied by a set of explanatory notes which expand on the meaning of the various principles.²⁵⁹

The Insurance Bureau of Canada adopted the *Model Privacy Code for the Individual Customer* in 1992, which was based on the OECD guidelines and was similar in many of its details to the 1990 CBA code. The 1992 code set out principles relating to specifying the purpose of personal information, the quality of personal information, the collection of personal information, the limitation of use of personal information, security safeguards, the individual right of access to personal information, accountability and openness. Complaints were to be resolved by procedures established by individual insurers.²⁶⁰

Later, the IBC decided to revise its model code based on the 10 principles of the CSA code. The new IBC code – known as the *Model Personal Information Code* – was approved by the Quality Management Institute of Canada as complying with the CSA code in 1997.²⁶¹ The new IBC code contains a variety of notable features in its statement of the consent, use limitation and access principle. The consent principle states that the individual may withdraw consent to the use of personal information on reasonable notice, subject to legal or contractual restrictions “and the

²⁵⁹ A few features of the new CLHIA guidelines deserve discussion. The collection limitation principle suggests that where “appropriate” information should be collected from the individual and that the individual should be notified before information is collected from another source. However, this principle does not apply to group insurers, since they cannot control the manner in which employers collect information about their employees. The use and disclosure principle states that information will be used in the manner that has been specified to the individual when it was collected, or in one of four other specific ways. The principle relating to access to information applies to all information in the insurance company's records, without the distinction between factual and opinion records made in the first CBA code. The code permits an insurance company to charge a reasonable fee for access and states that some medical information may be available only through the individual's doctor.

²⁶⁰ Several other provisions of the 1992 IBC code deserve to be highlighted. The purpose specification principle set out a list of purposes for which personal information could be collected that was tailored to the insurance industry, and so included: underwriting risks on a prudent basis, investigating and paying claims, and compiling statistics. Personal information was to be collected primarily from the individual but might include one of a number of external sources particularly relevant to insurers (such as brokers, the Insurance Crime Prevention Bureau and underwriting information networks). An insurer was to obtain personal information with the individual's consent, except in “exceptional circumstances, where there are reasonable and probable grounds for suspecting fraud.” On the use limitation principle, the IBC code set out a longer list of reasons for which information may be disclosed without the customer's consent than the 1990 CBA Code. The reasons included transferring information to other companies which share in the risk, transferring information for underwriting or claims purposes, and transferring information to insurance intermediaries. On the access principle, the IBC code followed the 1990 CBA Code's approach of permitting access only to factual information about the individual. Finally, the IBC code set out a suggested dispute resolution method for refusals of access: it stated that a customer wishing to challenge a refusal should send a letter to the president of the insurance company. The company then had a duty to “promptly institute a dialogue” with the customer and jointly agree to another method of dispute resolution if the dialogue fails.

²⁶¹ “IBC privacy code first to earn approval by CSA quality registrar,” in *Insurance Bureau of Canada Comment* (March 1997) at 1.

requirement that P&C insurers maintain the integrity of the statistics and data necessary to carry on their business.”²⁶² The use limitation principle states that there are several situations specific to the property and casualty insurance business where insurers will disclose personal information to others “as dictated by prudent insurance practices.”²⁶³ And the access principle raises the possibility that an independent mediation process will be available to individuals if a property and casualty insurer refuses access to the customer’s own personal information.²⁶⁴

Life insurance companies have adopted privacy policies based on the CLHIA guidelines and the IBC codes.²⁶⁵ London Life’s *Right to Privacy Guidelines* follow the CLHIA model, while The Mutual Life Assurance Company of Canada’s *Code of Business Conduct: Relations with Clients* includes privacy provisions. However, an articling student assigned the task of obtaining privacy brochures or codes from several other insurers was unable to do so. A representative of the Aetna Life Insurance Company informed the student that the company has guidelines based on the CLHIA guidelines, but that they are not available to the public. Other insurance companies did not return calls, indicated that their companies apparently did not have privacy codes or failed to provide the student with materials.

Over 80 property and casualty insurers or groups of insurers representing almost 75 per cent of the market (in terms of premiums) have adopted the 1992 IBC model code.²⁶⁶ Since the IBC 1992 code was intended to be adopted without amendment, these companies have made a commitment to using the code without publishing their own brochures or policies.²⁶⁷ It is expected that IBC members will soon adopt the 1997 version of the code.

²⁶² Insurance Bureau of Canada, *Model Personal Information Code* (1996), s 4.3.10. Several other notable provisions appear in the IBC code’s consent provision. The consent provision sets out unique features of the property and casualty insurance industry that make it impossible to obtain express or written consent in certain situations, such as the fact that such insurers operate through independent agents or brokers. It states that if an individual refuses to provide information about his or her date of birth, address and claims history, the insurer may refuse to provide insurance because the insurer will not be able to determine the appropriate rate. It states that one individual may consent to the collection and use of personal on behalf of multiple insured persons, as in the case of a person applying for auto insurance coverage for his or her family. And it states that for certain types of sensitive personal information – such as medical or hospital records, employment records or tax returns – express and written consent will always be obtained from the individual. See, respectively, ss. 4.3.1, 4.3.5, 4.3.8, and 4.3.6.

²⁶³ These include: disclosure of personal information to reinsurance companies that share in the risk; disclosure of personal information for underwriting, claims, classification or rating purposes; and disclosure of personal information to insurance intermediaries such as brokers and agents. See IBC 1996 model code, *supra*, note 262, s 4.5.1.

²⁶⁴ The access principle states that an insurer must provide the customer with information about how to challenge a denial of access to personal information, including: “(a) an invitation to the customer to send a letter to the [insurer’s] President requesting reconsideration of such denial; (b) a commitment by the [insurer] to open promptly a dialogue with the customer; and (c) a commitment by the [insurer] to participate in an independent mediation process should the parties be unable to resolve the dispute.” See IBC 1996 model code, *supra*, note 262, s. 4.9.1.

²⁶⁵ One observer has noted that large health and life insurers first published privacy guidelines or business codes which dealt with privacy in the 1980s. See Bennett, *supra*, note 219 at 29.

²⁶⁶ Fax sent by Steven Lingard of the Insurance Bureau of Canada to T.S. Onyshko on May 22, 1998.

²⁶⁷ Interview by T.S. Onyshko with Steven Lingard of the Insurance Bureau of Canada on February 20, 1998.

Credit Union Central of Canada

The Credit Union Central of Canada (CUC) is in the process of developing a model privacy code for member credit unions, which is expected to be implemented by late 1998.²⁶⁸ The CUC's draft model code is based on the CSA model privacy code and sets out the same general principles.²⁶⁹ However, there are several notable features to the CUC draft model code. The principle requiring that a credit union identify the proposed uses of information at the time that information is being collected from the individual states that the identified purposes should be "specific" to the individual.²⁷⁰ The principle requiring customer consent contains some discussion of the reasonable expectations of the customer in particular situations;²⁷¹ as well, the consent principle gives the individual the ability to withdraw consent, subject to contractual and other restrictions.²⁷² The principle on the use, disclosure and retention of personal information contains a special provision which discusses the treatment of health information; it suggests that health information may be used for both credit applications and related insurance purposes.²⁷³ And the principle on compliance raises the possibility that an individual unsatisfied with the credit union's complaint procedures may obtain a hearing before an independent mediator or arbitrator.²⁷⁴

Observations on Association Codes

A number of observations may be made about the way that the codes as a group might be improved to better meet the benchmarks provided by the OECD principles and privacy theory.

²⁶⁸ Letter from Susan Murray, Director of Government Affairs, Credit Union Central of Canada, to R.C. Owens, dated November 28, 1997.

²⁶⁹ Credit Union Central of Canada, *Credit Union Code for the Protection of Personal Information* (Draft) (June 1996).

²⁷⁰ *Ibid.*, s. 2.3. Presumably, this means that the written or oral explanation given to the individual must be tailored to some degree to the individual's circumstances. The draft model code goes on to suggest, for example, that an application form with the relevant purposes highlighted would meet this requirement.

²⁷¹ "In obtaining consent, the reasonable expectations of the member are also relevant. For example, a member who requests debit card services should reasonably expect that the credit union, in addition to using the member's name and address for statement mailing purposes, would also contact the member to renew the card. Similarly, consent will not be obtained when personal information is supplied to agents of the credit union to carry out processing functions, such as data processing or the printing of cheques. In this case, the credit union can assume the member's request constitutes consent for the specific purposes. On the other hand, the member would not reasonably expect that personal information given to a credit union would be given to a company selling insurance products, unless consent was obtained." CUC draft code, *supra*, note 269, s. 3.5.

²⁷² In a provision similar to that used in the CBA and IBC code, the CUC draft model code states: "A member may withdraw consent at any time, subject to legal or contractual restrictions, provided that: (a) reasonable notice of withdrawal of consent is given to the credit union; [and] (b) consent does not relate to a credit product requiring the collection and reporting of information after credit has been granted." See: CUC draft code, *supra*, note 269, s. 3.7.

²⁷³ "The [credit union] member's health records at the credit union may be used for credit application and related insurance purposes. The member's health records will not be collected from, or disclosed to, any other organization." See: CUC draft code, *supra*, note 269, s. 5.4.

²⁷⁴ *Ibid.*, s. 10.3. The draft code states that complaints not resolved by the credit union's designated official may be taken to the credit union's board of directors. If the complaint is not resolved by the board of directors, the credit union will have procedures to refer the complaint to Credit Union Central, a regulator or an independent mediator or arbitrator "as may be appropriate."

First, the codes generally permit the use of implicit consent, either by defining consent to include implicit consent or by failing to exclude implicit consent. Privacy theory's emphasis on individual control of information suggests that express consent should be the preferred form, particularly in cases where the information is sensitive. Some of the codes recognize that express consent should be preferred and that for certain types of information express consent should be required.²⁷⁵ However, it would be preferable for the codes to clearly limit the use of implied consent to non-sensitive information or to provide further guidance as to the circumstances in which implied consent is appropriate.

Second, the codes do not expressly address data mining and the use of personal information for targeted marketing purposes. To ensure that individuals retain some control over the use of personal information, it would be appropriate to permit them to opt out of data mining and targeted marketing programs. The model codes contain provisions which may apply to data mining and marketing uses of personal information. For example, the codes generally require that information be used for the purposes for which it was collected or that individual consent be obtained; as well, some of the codes state that an individual may later withdraw his or her consent to the use of information, subject to certain restrictions.²⁷⁶ The CBA code requires a bank to obtain consent from the individual to use information for marketing purposes.²⁷⁷ However, it would be preferable for the codes to state expressly that individuals may request institutions to refrain from using personal information for data mining and targeted marketing. Some financial institutions may not yet have information systems which permit them to remove selected individuals from their marketing lists. To avoid imposing undue costs on such institutions, the codes might impose a duty on institutions to make reasonable efforts to comply with the individual's request.

Third, the codes address the question of the purposes for which information may be collected with provisions that vary from code to code. Some codes state that information may be collected only if it relates to purposes stated in the code; other codes state that information must be "pertinent" to the business of the institution or "necessary for the purposes" that have been identified by the institution. To better meet the OECD principle of collection limitation, the codes might provide a more specific description of the types of information that may be collected – and perhaps a list of types of information that should not be collected. A related issue is when information may be collected from third parties rather than the individual. The codes might provide more discussion of the circumstances in which collection from third parties is appropriate. They also might require the institution to provide the individual with notice if the institution obtains a credit report about the individual.

²⁷⁵ The CBA code recognizes that express consent is the preferred form, while the IBC code states that express consent is required before the institution collects medical or hospital records, employment records or income tax returns. See: CBA 1996 model code, *supra*, note 244, s. 3.3 and IBC 1996 model code, *supra*, note 262, s. 4.3.6.

²⁷⁶ The CBA code, the IBC code and the CUC draft code recognize that a customer may later withdraw his or her consent to the use of information, subject to some restrictions. See: CBA 1996 model code, *supra*, note 244, s. 3.5; IBC 1996 model code, *supra*, note 262, s. 4.3.10; and CUC draft code, *supra*, note 269, s. 3.7.

²⁷⁷ CBA 1996 model code, *supra*, note 244, s. 5.3.

Fourth, the codes generally provide an open-ended list of reasons for which an individual may be refused access to his or her file: that is, the codes recognize that information may be refused (sometimes the codes add for “specific” or “valid” reasons) but do not set out the specific grounds for refusal. A list of specific exemptions is included in the access and privacy legislation applying to Canadian and provincial governments. It might be preferable for the codes to provide a list of specific types of exemptions, rather than leaving the list open-ended, although a case can be made for the flexibility afforded by the existing provision.

Finally, there are two further issues relating to the implementation of the model codes. First is the question of whether individual financial institutions provide copies of their codes to the public. As noted above, an articling student assigned to gather copies of privacy codes from different institutions had difficulties obtaining materials from some small banks, trust companies and insurance companies. In order for a system based on codes to work properly, the public should have access to such codes with relative ease. Individual institutions, industry associations and, if necessary, regulators, should take measures to ensure that the public may have access to the privacy codes of all financial services providers. We understand that proposed draft regulations under federal legislation will address this concern by placing a duty on financial institutions to provide information about their privacy policies to individual customers.

Second is the question of the review of consumer complaints made under the codes. The CBA model code is praiseworthy in that it gives the individual the ability to take an unresolved privacy complaint to the Canadian Banking Ombudsman. Other codes raise the possibility that a third party (such as a mediator) may be involved in the resolution of difficult complaints. From the point of view of privacy protection, it would be preferable for all industry associations to provide a means of review of privacy complaints similar to the Canadian Banking Ombudsman or some method of mediation. However, there is the question of the costs involved in such a system; the costs imposed on the industry to create review mechanisms may exceed the benefits that would be obtained. The question of review mechanisms will be discussed further in the conclusions to this study (Parts VI and VII).

These observations do not represent significant shortcomings but rather areas for potential improvement against ideal notions of privacy protection. It is important to recognize that the codes represent a significant commitment to privacy principles. Each code addresses the privacy and information concerns identified by the OECD principles. Each code sets out a variety of reasonable privacy principles and establishes the individual’s right to request access to his or her information and to seek correction of that information where it is inaccurate. The codes represent the basis for a reasonable system of self-regulation which has been established by the main industry associations for the financial services sector.

III. Privacy Challenges

Introduction

Part III discusses potential challenges to the protection of personal privacy. The Part begins by reviewing the key concerns raised by some privacy experts and consumer groups. These consist of the sharing and use of personal information, the use of implicit (as opposed to explicit) consent, the nature of dispute resolution systems and the openness of institutions, and the fact that various financial services providers are not regulated by federal legislation. The Part then considers technologies and trends with privacy implications: data aggregation, targeted marketing and data mining, stored value cards, Internet banking and money management software, international sharing of information and international provision of financial services.

Consumer Concerns²⁷⁸

Sharing and Use of Personal Information

As financial institutions provide a greater range of products and services and continue to improve their direct marketing programs, it can be expected that they will make greater use of personal information. The use of personal information to “target market” or “relationship market” is one of the big trends of retailing, and we would expect financial services to increasingly rely on it, like other retailers. Financial institutions, as information technology intensive industries, are perhaps near the vanguard of the trend. The positive way of looking at this is that banks are increasing their ability to provide personalized service. However, consumer groups and some privacy experts contend that the increased use and manipulation of personal information raises significant concerns relating to privacy and autonomy. At the extreme, it is contended that information could be used to manipulate or intimidate customers. For example, the Consumers Association of Canada has suggested that individuals might feel implicit pressure to accept new services offered by a bank through targeted marketing.²⁷⁹ The argument runs that the individual

²⁷⁸ For a discussion of consumer concerns, see, for example: Consumers' Association of Canada, *Privacy and Data Protection: Background Paper* (Ottawa: Consumers' Association of Canada, July 1992); Consumers' Association of Canada, *Consumer Data Protection* (Ottawa: Consumers' Association of Canada, March 1993); Consumers' Association of Canada, *Privacy in the Age of the Information Highway* (Ottawa: Consumers' Association of Canada, March 1995); Ed Pawlusiak, *Codes, standards and practices: Do they protect consumer interests?* (Ottawa: Consumers' Association of Canada, April 1996); Option consommateurs, *Les Canadiens et la protection des renseignements personnels détenus par les entreprises: éléments d'une législation (summaire d'une étude à paraître)* (Montreal: Fédération nationale des associations de consommateurs du Québec and Option consommateurs, February 1998); Association coopérative d'économie familiale du Centre de Montréal, *Les consommateurs et l'examen de 1997 de la législation régissant les institutions financières: Observations présentées au ministère des Finances du Canada* (Montreal: Association coopérative d'économie familiale du Centre de Montréal, 1996). See also the letter submission of Richard D. Speers of Toronto to the Task Force on the Future of Canadian Financial Services, dated September 23, 1997, in which Mr. Speers discusses various concerns relating to bank practices and privacy codes.

²⁷⁹ See, for example: Consumers Association of Canada, *Reform of Financial Services: Retailing of Insurance by Deposit-Taking Institutions* (August 1995).

will feel obliged to accept new products offered to him or her in order to maintain the relationship with the bank and so ensure access to future essential services, such as future credit.

Along with the general concern about increased use of information, consumer advocates have expressed particular concern about the use of insurance information by banks. As the ability of banks to offer insurance products through subsidiaries has expanded, new opportunities to use information gained through insurance activities may become available. The Consumers Association of Canada has argued that insurance information should not be used to make decisions about the individual's banking services.²⁸⁰ For example, the decision to deny insurance coverage to an individual should not be used to reduce the individual's credit rating. In addition, information about a potential health problem revealed to an insurer as part of the individual's duty of disclosure to the insurer should not be used against the individual when he or she later applied for a loan.

These concerns deserve closer examination. Marketing programs can involve intrusion by unsolicited telephone calls or unsolicited mail.²⁸¹ However, marketing programs may have the actual benefit of bringing useful products and services to the attention of consumers with particular needs or interests. While "data mining" and target marketing have proven to be useful technologies from the marketer's point of view, it is not correct to suggest that they have any capability to unduly influence individuals or are intended to do so. Furthermore, under existing privacy codes, banks and insurers have committed themselves to the principle that an individual may later withdraw his or her consent to the use of personal information for particular purposes.²⁸² Increasing sophistication of financial services systems may permit such consent to be withheld in respect of specific categories of services.

There is a reasonable argument that medical information collected for insurance purposes should not be used for making decisions about banking services, particularly when banking services have traditionally not involved a review of such information. Financial and health information are among the types of information considered most sensitive by the public, and there may be legitimate policy objectives involved in keeping some distance between the two types of information.²⁸³ The Canadian Bankers Association model code specifically deals with this issue, stating that health records will be collected only for specific purposes, and that banks and subsidiaries will not disclose health records to each other.²⁸⁴ In general, the institution is better

²⁸⁰ *Ibid.*

²⁸¹ Certain types of telephone solicitations are regulated by the CRTC on privacy grounds, privacy being an express policy to be applied in the interpretation of the new *Telecommunications Act*. The Canadian Direct Marketing Association voluntary code imposes limits on unsolicited mail from the Association's members.

²⁸² The model codes of the Canadian Banking Association and the Insurance Bureau of Canada permit the individual to withdraw his or her consent subject to certain restrictions. As well, the CBA code requires banks to obtain individual consent before using personal information for marketing purposes. See footnotes 276 and 277 in Part II and accompanying text.

²⁸³ Ekos Research Associations Inc., *Privacy Revealed: The Canadian Privacy Survey* (Ottawa: Ekos Research Associates, 1993) at 20. For further discussion of the Ekos Survey, see Part I of this study under the heading Public Concern About Privacy and Privacy Complaints.

²⁸⁴ Canadian Bankers Association, *Privacy Model Code: Protecting individual bank customers' privacy* (1996), Principle 5.

served by collecting only the information necessary to its credit decision. Institutions are required to have, and follow, internal credit policies to discipline the credit investigation and granting process. Such policies would not be served by considering extraneous information of uncertain relevance taken in another context. Moreover, insurers, including insurers which are owned by other financial services providers, have an essential interest in accurate information disclosure by insured.²⁸⁵ In particular, insurers rely on the doctrine of *uberrimae fides*, or the duty of highest good faith, which provides that an insured owes a duty to disclose to the insurer all relevant information requested by the insurer in respect of a policy. Implicit in that obligation is the obligation of the insurer to act as a steward of that information. The insurer most certainly would not want to discourage such disclosure by being known to be in a position of inappropriately using information provided. After all, there are generally no restrictions on what can be asked with respect to a credit application, provided the information is relevant. It is better for a lender to ask for information again, even if it duplicates information obtained in the insurance context, than it is to rely on other, perhaps older records obtained in a different context and under different conditions.

An issue commonly raised in discussions of informational privacy is the transfer and use of personal information outside the collecting institution. However, this issue appears to have less relevance in the context of regulated financial institutions. Such institutions are under a statutory duty to protect customer information and have a long tradition of maintaining the confidences of their customers.²⁸⁶ In addition, such institutions are presumably subject to the implied duty of confidentiality recognized in the *Tournier* decision.²⁸⁷ Although that decision applies directly to banks, there is no basis for distinguishing other financial services providers on principle. Unauthorized transfers or disclosures outside regulated financial institutions are illegal and would certainly be counter-productive to the business of the institution if they became public knowledge. In general, transfers or disclosures outside financial institutions will occur only with the customer's explicit or implicit consent. For example, banks routinely provide customer's credit information to credit bureaux, but consent to such disclosure will be provided for on the form that the customer completes to apply for the bank service.²⁸⁸ Moreover, there is a compelling social need to ensure that this disclosure takes place, so that businesses which

²⁸⁵ Interestingly, they do not have an interest in knowing everything. As is ably demonstrated by the economic analysis set out in an unpublished paper by Trevor Hoffman, "The Economics of Privacy: an analysis of information access in the insurance context" (1997), in a world of perfect knowledge, the entire insurance enterprise would fail because premiums would equal the marginal cost of every risk. It is only the ability to actuarially spread risk over a large population that permits the insurance market to go forward.

²⁸⁶ For discussion of the provisions relating to privacy and customer information in federal legislation and regulations, see Part II of this study under the heading Legislative Provisions Respecting Financial Institutions and Confidentiality.

²⁸⁷ For discussion of the *Tournier* decision, see Part II under the heading The Implied Contractual Duty of Privacy. *Tournier* was a case about a bank and similar cases recognizing an implied duty of confidence also involve banking institutions, presumably because banks are most frequently contacted for credit references and the like. However, there appears to be no basis on which to contend that *Tournier* should not apply to other financial institutions holding confidential information. In fact, we would suggest that the implied duty of confidence will apply similarly to unregulated institutions, such as consumer credit companies.

²⁸⁸ See, for example, the discussion of bank account opening forms in Part II at footnotes 136 to 140 and accompanying text.

provide credit may assess an applicant's credit history. Unauthorized transfers or disclosures of personal information *occasionally* do occur, as complaints to the Canadian Banking Ombudsman and the Commission d'accès à l'information du Québec suggest.²⁸⁹ But these situations are the result of mistakes or misunderstandings by bank staff, and do not represent normal bank practices.

Implicit v. Explicit Consent

Another issue is the question of implicit as opposed to explicit consent. Consumer groups and some privacy experts take the position that in order for an institution to use an individual's personal information, the institution should obtain the individual's explicit consent.²⁹⁰ Furthermore, when an institution is obtaining an individual's consent, the institution should require that the individual "opt in" to such uses of information by a positive action (for example, by ticking a box that describes the institution's proposed use of information). Consumer groups and some experts argue that the alternative – requiring an individual to "opt out" before the institution will refrain from using the information as proposed – does not provide a sufficient degree of privacy protection. Put another way, they contend that the protection of privacy should be the rule and any proposed use of personal information should be treated as an exception which requires the individual's consent through some positive act.

In contrast, industry privacy codes state that consent to the use of personal information may be implicit. For example, the Canadian Bankers Association 1996 code states: "A customer's consent can be expressed, implied or given through an authorized representative."²⁹¹ The CBA code states that while express consent is the "preferred form," a bank may imply consent from the customer's use of a bank product or service, or from the customer's failure to respond to an offer by the bank to have the individual's information removed from a marketing list. But the CBA code adds that before deciding what type of consent is appropriate (i.e., oral or written, express or implicit) the bank will consider the type of personal information, the reason for its use and the type of customer contact involved. The CSA model code also recognizes the possibility of implied consent, stating that the form of consent should vary depending on the circumstances and the type of information.²⁹² While the value of explicit consent is not denied, sometimes explicit consent is more important than others. Not all potential and necessary uses of personal

²⁸⁹ See the discussion of complaints to the Canadian Banking Ombudsman and the Québec access and privacy commission in Part I of this study under the heading Public Concern About Privacy and Privacy Complaints.

²⁹⁰ See, for example, Consumers' Association of Canada, *Privacy, Data Protection and Financial Institutions: Submission of the Consumers' Association of Canada to the Senate Standing Committee on Banking, Trade and Commerce* (Ottawa: Consumers' Association of Canada, 1992) at 3: "Consumers have a fundamental right to information self-determination. It is consumers who should decide if they want their information used. This concept which CAC heartily endorses is known simply as 'positive consent.'"

²⁹¹ CBA 1996 model code, *supra*, note 284, Principle 3.

²⁹² The CSA code states that when information is likely to be considered sensitive, express consent should be sought; however, where information is less sensitive, implicit consent may be sufficient. As well, when obtaining consent, it is relevant to consider the reasonable expectations of the individual. Presumably, if the reasonable expectations of the individual would not include a particular use of personal information, then express consent would be appropriate. See: Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada*, CAN/CSA-Q830-96 (Etobicoke, Ont.: CSA, 1996), Principle 3.

information can be anticipated in a request for consent. Such subsequent uses as may arise might not implicate such interests as to make going back for explicit consent at all worthwhile. If they do, and institutions ignore those interests, the marketplace will provide motivations to upgrade their standard of behaviour.

Given that at least some types of personal information may not raise significant privacy concerns, a flexible approach to consent seems reasonable. The key concern seems to be to ensure that appropriate judgment is used to determine when implied consent is appropriate. One might expect that if the choices made by financial institutions do not accord with the expectations of most individuals, there will be a public outcry leading regulators to intervene. Furthermore, the precise manner in which consent is obtained may be less relevant if the customer is given an opportunity to withdraw their consent at any time in the future. As noted above, many financial institutions have committed themselves to the principle that, with certain exceptions, an individual should be able to withdraw his or her consent to the use of personal information. Finally, the “opt out” approach to obtaining customer consent may be legitimate if the majority of customers could be expected to consent. The low level of privacy complaints made by customers of financial institutions suggests that this may be the case.

Dispute Resolution Systems and Openness

Another issue raised by consumer groups and some privacy experts relates to the dispute resolution mechanisms for complaints made under the privacy codes of financial institutions. Such codes generally call for complaints to be resolved by procedures adopted by the financial institution itself. Consumer groups and some experts question whether these mechanisms provide appropriate and effective forms of review. As a result, they propose that consumers have an ability to bring their complaints to an independent, government review agency, with the power to enforce its decisions on financial institutions.²⁹³

Concerns of bias arise about relying on procedures that are internal to an institution to resolve complaints. An internal official may possess a high degree of autonomy, but still share the general outlook of the institution or face implicit pressure to decide certain matters in certain ways. However, the concern seems less serious when a review process located outside the institution is also available. Some industry codes make provision for a degree of external review. The code of the Insurance Bureau of Canada raises the possibility of mediation before an independent mediator in the case of a denial of access to the customer’s own information.²⁹⁴ The model code of the Canadian Bankers Association states that customers who are unsatisfied

²⁹³ See, for example, *Privacy, Data Protection and Financial Institutions: Submission of the Consumers’ Association of Canada to the Senate Standing Committee on Banking, Trade and Commerce*, *supra*, note 290, at 5: “Even if privacy codes become a feature of the Canadian marketplace, their effectiveness to protect an individual consumer’s privacy remains in doubt. CAC’s position has been, and continues to be, that consumers are not able to protect their own privacy without the assistance of regulatory authorities. This includes the need to develop an effective mechanism for monitoring compliance.”

²⁹⁴ Insurance Bureau of Canada, *Model Personal Information Code* (1996), s. 4.9.1.

with the bank's handling of a complaint may complain to the Canadian Banking Ombudsman.²⁹⁵ The banking industry appears to have the most developed complaint handling process, with internal ombudsmen or complaint officers providing a first stage of review and the Canadian Banking Ombudsman providing a second stage.

The exact degree of independence of the Canadian Banking Ombudsman may be open to debate.²⁹⁶ On the one hand, the office of the Ombudsman was established by the banking industry, is responsible to a board composed in part of bank representatives, and does not have the power to force a bank to follow his recommendations. On the other hand, the Ombudsman is not beholden to any particular bank, has a mandate to operate as an independent investigator and mediator of disputes, and may be able to ensure that his recommendations are followed by applying moral pressure and the threat of negative publicity. The limited experience to date suggests that the Ombudsman will make recommendations that are in the interests of complainants.²⁹⁷ However, at this early stage in the development of the Ombudsman's office, it does not seem possible to accurately assess its effectiveness. A final thought is that there may be more willingness within the banking community to comply with the recommendations of an industry-established Ombudsman than the orders of a government-imposed review agency. It is worth noting, too, that while it might be arguable that there is an industry bias in the bank ombudsman, the fact that he represents the interests of all the major banks means that, in respect of any particular issue, all the members of his board but one have a competitive interest in embarrassing the institution involved.

In addition to the particular concern about the independence of complaint resolution mechanisms, there is the more general concern of the openness of institutions about their information practices and privacy policies. Industry codes include the principle that institutions should be open about such matters and also, in general, require institutions to provide specific information about privacy policies and complaint mechanisms. Obviously, such openness about consumer benefits is in the interest of the institution. However, a legitimate concern will arise if such information is not easily available in practice. There may be problems of this nature involving some sectors of the financial services sector. An articling student assisting with this study was assigned the task of gathering privacy codes and policies faced significant difficulties in obtaining such information from some small banks, some trust companies and some insurers.²⁹⁸ In several cases, his phone calls were not returned and his questions about such materials went unanswered.

²⁹⁵ CBA 1996 model code, *supra*, note 284, Principle 10. In addition, Insurance Bureau of Canada's code raises the possibility of an independent mediation in the case of a denial of access to personal information, and the draft Code being considered by Credit Union Central of Canada suggests that complaints not resolved by internal procedures within a credit union should be referred to the Association or an independent mediator or arbitrator. See: IBC model code, *supra*, note 294, s. 4.9.1; Credit Union Central of Canada, *Credit Union Code for the Protection of Personal Information (Draft)* (1996), Principle 10.

²⁹⁶ For information about the Office of the Canadian Banking Ombudsman, see: Canadian Banking Ombudsman, *Annual Report 1996*, and Canadian Banking Ombudsman, *Report for the nine months ended July 31, 1997*.

²⁹⁷ See: Canadian Banking Ombudsman, "Privacy Case Summary" (November 17, 1997), a short document provided by the Ombudsman to the authors of this study. Of the two cases resolved by the Ombudsman as of November 1997, the bank involved paid \$4,000 and \$500 in order to settle the complaints on the recommendation of the Ombudsman.

²⁹⁸ For further discussion, see Part II under the heading Industry Association Codes.

Moreover, in some cases, he was informed that the institution did not have a privacy code, that the representative did not know of any privacy code, or – most unusual of all – that the insurance company had a privacy code but it was not available to members of the public.

Entities Not Regulated by Federal Legislation

A final consumer concern is that many entities that offer financial services are not subject to the same legislative duties and scrutiny as federally regulated institutions. Regulated banks, insurance companies and trust companies face pressure from federal regulators to adopt privacy codes; moreover, new regulations are expected in the near future to require such institutions to adopt codes. Provisions in federal legislation and regulations also require policies relating to the confidentiality of customer information.²⁹⁹ However, many entities that offer financial services in competition with banks, insurance companies and trust companies are largely unregulated. For example, consumer finance companies which fall outside federal financial legislation may offer credit to the public. While they must comply with provincial legislation relating to credit generally, such companies will not be subject to the privacy provisions of federal legislation nor the scrutiny of federal regulators. Thus, companies offering some services similar to those offered by federally-regulated institutions may have lower levels of privacy protection for customers – a fact that may be unknown to the average consumer. However, it should be noted that such institutions typically have less sensitive information than would, for instance, a bank or insurer. As well, some representatives of the consumer finance industry do have privacy policies, although we are not aware of how common such policies are in the non-federally regulated sector. In any event, we are not aware of any empirical evidence of a level of privacy problems in the sector which would reinforce any recommendation for further regulation.

New Technologies and Trends

Data Aggregation

As financial institutions become larger and offer a wider range of services and products, they are changing the ways that they store and assess their information. Traditionally, customer data was stored in separate “data silos” – accumulations of data which were relevant to a particular division of the institution or a particular set of products or services but which were not accessible throughout the institution. Thus, for example, an individual’s deposit account information might be stored in one silo while an individual’s investment records might be stored in another. As different divisions have been added to financial institutions and as these institutions have sought to have these divisions work in a more integrated fashion, the concept of the “data warehouse”

²⁹⁹ For discussion of the provisions relating to privacy and customer information in federal legislation and regulations, see Part II of this study under the heading Legislative Provisions Respecting Financial Institutions and Confidentiality.

has replaced the data silo.³⁰⁰ Ideally, institutions wish to store data in a format that can be accessed across the institution and used for a variety of different purposes with minimal effort. This may involve new computer hardware systems that share data more effectively and new computer software that allows staff in different divisions to obtain a comprehensive picture of an individual's dealings with the institution. The institution's data warehouse could be used in a variety of ways. For example, it may permit the institution to update the customer's address once, rather than at each point of access between the individual and the institution, or to provide better service to customers traveling from city to city. In addition, the institution might use "data mining" techniques to analyze the collected customer information and so gain an understanding of how to better design products for its customers.

Arguably, even if personal information continues to remain within financial institutions, privacy may be threatened as a greater number of uses are made of personal information. This raises informational privacy concerns about the relationship of the institution and the individual similar to those discussed above.³⁰¹ However, once the policy choice has been made to permit the same institution to offer a wide variety of products and services through its divisions, it seems counterproductive to impose measures designed to enforce a rigid separation of those divisions. Institutions naturally seek to increase the efficiency, flexibility and integration of their information systems. Amongst other benefits, this allows them to better market products to their customers and design products for them. The privacy concerns involved in the increased use of personal information are real, but they must also be evaluated in the light of the practical benefits both to the institutions and to their customers.³⁰²

Targeted Marketing and Data Mining

Targeted marketing and "data mining" will play an important role in the future activities of financial institutions. Targeted marketing is the notion that an institution should focus its marketing efforts to those most likely to accept a product or service.³⁰³ Rather than undertake a mass marketing program aimed at all the institution's customers, the institution should focus on a smaller segment with the needs or inclinations relevant to a product or service. A person's past history of transactions with the institution, as well as his or her assets and income levels, may be relevant to determining an individual's likely needs or interests. For example, a customer with a large amount of money in his or her savings account may be interested in investment dealer services, while a customer who has taken out a mortgage may be interested in insurance for the

³⁰⁰ "Data Warehousing is the strategy of ensuring that the data used in an organization is available in a consistent and accurate form wherever it is needed. Often this involves the replication of contents of department computers in a centralized site, where it can be ensured that common data definitions are in use...." Michael Bell, *A Data Mining FAQ*, at <http://www.qwhy.com/dmfaq.htm>.

³⁰¹ See the discussion in this Part III under the heading Consumer Concerns and the sub-heading Sharing and Use of Personal Information.

³⁰² In any event, it should be remembered from a practical perspective the day of the data warehouse has not yet arrived. In reality, most institutions are faced with a variety of incompatible systems borne of specific business initiatives and discretionary technologies spending over many years. While the ideal of data as available from any node in a wide area network is sought after, it may be many years before it is achieved.

³⁰³ For further discussion of targeted marketing, see, for example: Garth Hallberg, *All Consumers Are Not Created Equal: The Differential Marketing Strategy for Brand Loyalty and Profits* (New York: Wiley & Sons, 1995).

property. Using targeted marketing, an institution will direct its marketing efforts so that they are more cost effective. Individuals perceived as unlikely to have a need or interest for new products will receive less attention, while those perceived as likely to have such a need or interest will receive greater – and more personalized – attention. Personal information will form the basis for the decision about how to categorize a particular individual.

The concept of data mining is one that has come to prominence over the last few years and is certain to gain further importance in the future. Data mining is a set of techniques which are intended to reveal new connections, patterns or associations between different items of information. As one study defined the concept:

Data mining is a set of automated techniques used to extract buried or previously unknown pieces of personal information from large databases. Successful data mining makes it possible to unearth patterns and relationship, then use this “new” information to make proactive knowledge-driven business decisions. Data matching then, “centres on the automated discovery of new facts and relationships in data. The raw material is the business data, and the data mining algorithm is the excavator, sifting through vast quantities of raw data looking for valuable nuggets of information”.³⁰⁴

Unlike more traditional forms of analysis, data mining does not seek to answer a particular question by extracting relevant data from a database. Rather, data mining seeks to locate useful connections that may not be obvious to either the institution or the subject individuals. “[T]he data is sifted in search of frequently occurring patterns, trends and generalizations about the data without intervention or guidance from the user. ... The data is searched with no hypothesis in mind other than for the system to group the customers according to the common characteristics found.”³⁰⁵ Using data mining techniques, an institution might discover that if the individual has characteristics A, B and C but not D, the individual is more likely to want product or service X.

The advantage of data mining is that it frees marketers from predetermined approaches to their customers. As well, data mining has proven useful in the context of fraud prevention (e.g., data mining technology has been used to develop techniques to recognize anomalous credit card transactions). However, proper data mining is difficult to do and depends on the quality of both the software tools employed and the customer data that has been accumulated. Often, data mining yields information that is mundane, useless or wrong.³⁰⁶

Data mining has become possible as the cost of powerful computer equipment and sophisticated software has fallen and the volume of information collected by institutions has increased. In addition, data mining becomes easier as institutions move to consolidate their information holdings in central data warehouses that hold personal information in a standard and easily accessible form. Such techniques are used routinely by large corporations such as Blockbuster Entertainment, MasterCard International, American Express and WalMart.³⁰⁷ As Canadian

³⁰⁴ Ann Cavoukian, *Data Mining: Staking A Claim on Your Privacy* (Information and Privacy Commissioner/Ontario, January 1998) at 3, available at www.ipc.on.ca.

³⁰⁵ Queen’s University of Belfast, What is Data Mining at http://www.pcc.qub.ac.uk/tec/courses/datamining/stu_notus/dm_book_2.html#HEADING2, as cited in Cavoukian, *supra*, note 304.

³⁰⁶ Craig Stedman, “Data Mining for Fool’s Gold,” *Computerworld*, December 1, 1997, pp. 1 and 28.

³⁰⁷ Cavoukian, *supra*, note 304 at 6-7.

financial institutions adopt targeted marketing programs, data mining techniques will become more common in the financial services sector. Yet it seems likely that such techniques will not be well known among the customers unless positive measures are taken to inform them of the way their information is being used.

Targeted marketing and data mining are trends which raise interesting privacy issues. Both involve an increased use of personal information to make business decisions about individuals, and activities which may not be anticipated by individuals at the time the information is collected from them. In a recent analysis of the privacy implications of data mining, the Ontario Information and Privacy Commissioner pointed to a few key concerns.³⁰⁸ For example, data mining necessarily involves the use of large amounts of data. Unless care is taken by the institution, this data may include historical but now inaccurate personal information. Furthermore, it is suggested that a meaningful approach to data protection will require institutions to reveal their data mining operations at the time that information is collected from the individual. Otherwise, such operations may fall outside the expectations of the individual and be viewed as incompatible with the purpose for which the information was collected (i.e., to provide some product or service). However, to simply identify “data mining” as one of the potential uses of the information may not amount to meaningful disclosure by the institution or consent by the individual. On the other hand, the institution may not know the ultimate purposes that the data will be used for, since this may depend on associations that will be discovered only after the data mining process itself.

It is worth noting that the extent to which data mining affects the privacy interests of individuals is open to debate. Data mining involves the discovery of relationships among large quantities of aggregated data, which relationships are not related to identifiable persons. In the same way, the aggregation of large amounts of personal data into general population statistics does not reveal information about identifiable individuals. It might be said that no privacy interest is involved in either data mining or the compilation of general statistics. On the other hand, the next step after data mining usually is to apply the relationships recognized to particular individuals, in order to target market or otherwise make decisions about them. Accordingly, data mining may incidentally involve a privacy interest because it provides the institution with tools that will be applied to particular individuals, based on their particular, known characteristics to structure the relationship between the institution and the individual.

³⁰⁸ *Ibid.*, at 8-11.

Stored Value Cards

The first widespread implementation of “smart card” technology in the financial services sector will be in the form of the stored value card.³⁰⁹ A smart card is a card roughly the size and shape of a credit card, and contains embedded logic circuits and digital memory. Such a card may store a larger amount of information than traditional magnetic stripe cards; furthermore, the information stored on the card may be changed and updated each time the individual uses the card to accomplish some transaction. Over the next several years, it is expected that smart card technology will begin replacing traditional magnetic stripe cards in a variety of applications.

The stored value card (also known as an electronic purse) is intended to offer a convenient alternative to cash that may be used for all types of consumer purchases. The consumer obtains the card from the issuer and loads the card’s memory with a certain amount of value. The consumer then may make purchases from merchants who have machines that deduct value from the card;³¹⁰ in some systems, the consumer also may transfer stored value from one card to another. The degree of privacy in a stored value system varies with its design. In systems with greater privacy, records of purchases are kept only on the stored value cards and the merchants’ card readers; in other systems, detailed central records are kept by the card issuer.

Most major deposit-taking financial institutions are participating in the introduction of the Mondex stored value system in Canada. The system has been implemented in Guelph, Ontario and is expected to be made available across the country in the near future.³¹¹ Unlike other systems, Mondex is not centrally accounted and does not maintain detailed records in a central database. Records identifying the last 10 card transactions are stored on the card itself; records identifying the last 300 card transactions (identified only by a card number and not by identity of the cardholder) are stored on the merchants’ terminals.³¹² Merchants may print out paper copies of the transaction data, for use in the case of a future dispute. However, merchants will not know the identity of the cardholders who made purchases unless this information is supplied by the card issuer. Card issuers will not supply identifying information unless they are required to do so by law or the cardholder has agreed to participate in a customer loyalty scheme promoted by the

³⁰⁹ In addition to stored value cards, discussed below, smart card technology raises other questions for the future. Technical observers have noted that the same smart card could be used to provide a variety of unrelated services. For example, a single smart card might provide information about medical treatment, access to restricted areas on an employer’s premises and consumer financial transactions. A stored value card used for a variety of non-financial purposes would raise concerns about the ability of parties to gain access to sensitive information unrelated to the party’s own transaction with the individual. For further discussion of stored value cards see, for example: T.S. Onyshko and R.C. Owens, “Debit Cards and Stored Value Cards: Legal Regulation and Privacy Concerns” (1997) 16 *National Banking Law Review* 65.

³¹⁰ In addition to card readers located on the merchants’ physical premises, prototype devices exist that would allow consumers to make stored value purchases using a personal computer equipped with a modem.

³¹¹ See the Mondex International web site at <http://www.mondex.com> and the Mondex Canada web site at <http://www.mondex.ca>. Participants in the Mondex Canada system now include Canadian Imperial Bank of Commerce, Royal Bank, Hongkong Bank of Canada, Credit Union Central of Canada, Bank of Montreal, Canada Trust, Le Mouvement des caisses Desjardins, National Bank of Canada, The Toronto-Dominion Bank and Scotiabank.

³¹² See the Mondex International web site discussion of “How private is a Mondex transaction?” at <http://mondex.com> under the “About” and “Mondex FAQ” headings and the Mondex Canada web site at <http://mondex.ca/faq5.html>.

merchant.³¹³ Mondex provides a high degree of customer privacy but merchants and card issuers can with cardholder consent cooperate to create electronic databases of transaction information incidentally involving the Mondex card.³¹⁴

Some privacy experts have argued that anonymity is an essential part of a stored value system. A stored value system that functions as a replacement for cash without the anonymity of cash could generate a huge amount of information about an individual's movements and purchasing habits. One writer's observation on the need for privacy protection of Internet transactions also applies to the need for anonymity in a stored value system: "Without such protection, a third party could easily follow a user's every move, create a personal profile for commercial use, or learn the intimate details of a person's everyday life, all by tracing his financial transactions...."³¹⁵ However, this argument does not provide sufficient justification for regulating a stored value system in the absence of evidence of any problems. First, the Mondex system is a private one. Based on statements of the Mondex organization, the system will be used to collect information based on card purchases only if the customer has agreed to join an associated loyalty scheme. Thus, privacy will be the norm unless the consumer has consented to some particular use of his or her purchase information. Second, the Mondex system is more private than competing payment systems such as credit cards and debit cards, which collect detailed records of customer purchases. Just as there is no specific regulation applying to protect the privacy of credit card and debit card transactions, it does not seem necessary in the case of Mondex card records. Finally, it is not clear that the vast amount of information about day-to-day consumer purchases that might be collected through a centrally-accounted stored value system (unlike Mondex) would be useful. The cost involved in storing, sorting and analyzing the many millions of routine cash transactions might well exceed any the value of any useful data that could be derived from the operation.

Canadian Internet Banking and Money Management Software

In an attempt to offer new channels of distribution, Canadian banks and trust companies are offering PC-based and Internet banking services.³¹⁶ These services permit consumers to carry out banking transactions using a modem and home computer, rather than at a branch of the institution or an automated teller machine. For example, consumers might transfer money between accounts, pay bills or apply for personal loans through these services. In the future, it is expected that institutions will offer PC-based and Internet services compatible with popular personal accounting software such as Microsoft Money or Intuit's Quicken.³¹⁷ Thus, for example, customers might use accounting software to withdraw, deposit or conduct other

³¹³ *Ibid.*

³¹⁴ Interview by T.S. Onyshko with Mondex Canada spokesperson Joe Clark on September 8, 1997.

³¹⁵ Catherine M. Downey, "The high price of a cashless society: exchanging privacy rights for digital cash?" (1996) 14 *John Marshall Journal of Computer & Information Law* 303 at 315.

³¹⁶ See, for example, Michael Smith, "The Internet has landed" *Canadian Banker* (September-October 1997) 34; and Michael Smith, "Technology and Trust" *Canadian Banker* (November-December 1997) 35.

³¹⁷ See, for example, Kevin Marron, "Bankers edgy over software middlemen" *The Globe and Mail*, November 25, 1997, p. C-1.

transactions through PC-based and Internet services, and institutions might provide records of such customer transactions in a form that could be used by the accounting software.

The new PC-based and Internet banking services raise certain privacy concerns. One concern is that the services might be vulnerable to attack by unauthorized persons, who could change or delete banking information. An assessment of the security features of PC and Internet banking services is beyond the scope of this study. However, it is worth remembering that unauthorized access to information occurs in the physical world as well; thus, the aim is to reduce the possibility of unauthorized access to acceptable limits, rather than to completely eliminate it. Another concern relates to the fact that PC-based and Internet banking services may allow consumers to store their confidential banking information on their own personal computers. If such information is not encrypted or kept in "locked" files, it may be open to inspection by people with access to the individual's computer, such as friends or family. Here, it seems that individuals need reminders of the need to protect the confidentiality of electronic information in the same way as paper bank book records. The onus of taking the steps needed to protect electronic records would then rest on the individual. Improper security at the banking terminal end – the home PC – is likely a bigger risk than bank system failure.

International Sharing of Information and International Provision of Services

A final set of trends relates to the growing globalization of the market for financial services. In general, while these trends will see greater sharing of personal information and more processing of information outside of Canada, it is unlikely that they will pose a serious risk to privacy.

In the future, it is likely that Canadian financial institutions will cooperate more closely with foreign institutions. For example, Canadian institutions may enter into international joint ventures or other arrangements to implement new technologies and systems. One part of these new arrangements may be the sharing of customer information. We are not, however, aware at the moment that such sharing of information would exceed that which occurs in respect of credit cards: that is, such minimal sharing of information as is necessary to facilitate the convenient use of the card in a jurisdiction other than that of the issuer. (For example, the Mondex stored value system involves the international sharing of information relating to stored value purchases made in other countries.) It seems certain that the contracts between institutions establishing these new arrangements will include provisions intended to protect the privacy of Canadian customer information. However, the implication of such arrangements is that personal information may be shared more widely, among a greater number of institutions in a greater number of countries.

It is also possible that Canadian financial institutions will process data outside the country in some other portion of their far flung empires, or with an outsource service provider in a different jurisdiction. Such processing can only occur at present for a federal institution provided the consent of the Office of the Superintendent of Financial Institutions is obtained under the relevant Act. The purpose of such consent is ostensibly to ensure the security of data and its availability in the case of the need for the exercise of regulatory control, but in any event such oversight substantially serves the privacy goal. The factors driving the location of data processing, particularly as flexibility of telecommunications services increases and the cost thereof declines, may increasingly face competitive pressures to occur in the lowest cost

jurisdictions (which may very well be Canada). Foreign owned unregulated service providers are more likely to process data offshore, in aggregation with their easier, home jurisdictions processing needs. Such institutions are more likely to process personal data outside the country, and they may or may not be subject to the privacy and confidentiality requirements of the *Bank Act* or other relevant federal legislation. Again, it is worth pointing out that we are aware of no empirical data of any difficulties with this sector.

A final problem might arise if a foreign corporation offered financial services to Canadians over the Internet, and then used the information it collected without regard to privacy principles. This situation would raise serious concerns but would be difficult or impossible to address given the jurisdictional limits of Canadian regulators. General regulatory concerns about the use of foreign financial services providers have been addressed in the recent Department of Finance consultation paper on foreign banks.³¹⁸ Except to the extent that foreign regulators are willing to cooperate to address a problem identified by their Canadian counterparts, it appears that the regulatory options are so limited that the rule is likely to be and remain *caveat emptor*.

³¹⁸ Government of Canada, Department of Finance, *Foreign Bank Entry Policy: Consultation Paper* (September 26, 1997), available at www.fin.gc.ca/toce/1997/foreigntoc-e.html.

IV. International Conventions, The EU Directive and Legislation in Foreign and Domestic Jurisdictions

Introduction

Part IV discusses international agreements and statutes that protect privacy in certain foreign and domestic jurisdictions. It begins by briefly reviewing international conventions and agreements involving Canada that provide for the protection of privacy. It then turns to a detailed discussion of the European Union's data protection directive; in particular, the discussion considers the restrictions on the international transfer of personal information imposed by the directive. The remainder of the Part discusses the private sector privacy legislation adopted in three jurisdictions and the experience of a fourth jurisdiction that decided against such legislation. The United Kingdom's *Data Protection Act*, 1994 provides an example of legislation that requires data users to register with a central authority. Quebec's *Act respecting the protection of personal information in the private sector* provides an example of a non-registration system with detailed privacy duties. New Zealand's *Privacy Act* 1993 provides an example of legislation that mixes statutory duties with approved private sector privacy codes. Finally, Australia provides an example of a jurisdiction that considered, and then rejected, an extension of data protection legislation to the private sector.

International Conventions and Agreements Involving Canada

Canada has acknowledged its commitment to protecting the privacy of its citizens by acceding to a number of international agreements. For example, Canada is a signatory to the *Universal Declaration of Human Rights*, which was adopted and proclaimed on December 10, 1948 by the General Assembly of the United Nations. Article 12 of the Universal Declaration specifically addresses the issue of privacy:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.³¹⁹

The Universal Declaration addresses such rights as the right of life, liberty and security of person, the right not to be detained arbitrarily, treated cruelly, or discriminated against, and the right to freedom of thought and religion. The fact that privacy is numbered among these rights is a clear indication of the importance which the international community attaches to privacy. It should be remarked, however, that privacy, in that pre-computer age, did not connote the kinds of informational privacy issues we primarily are discussing in this paper. Canada is also a signatory

³¹⁹ U.N.G.A. Res. 217 (III), 3 U.N. GAOR Supp. (No. 3) 71, U.N. Doc. A/810 (1948).

to the *International Covenant on Civil and Political Rights*,³²⁰ Article 17 of which is identical in wording to Article 12 of the Universal Declaration.

The *OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*³²¹ represent a more significant development in the international protection of privacy. In 1984, Canada formally adhered to the OECD guidelines thereby committing the federal government to the protection of individual privacy in the public and private sectors.³²² The guidelines, which are voluntary and thus have no legal force, are centred on eight principles of fair information practices which govern, among other things, the collection and disclosure of personal information and an individual's access to information relating to him.³²³ OECD member countries are expected to implement legislation which provides individuals with adequate sanctions and remedies in case data users fail to comply with the principles.³²⁴

EU Directive

The European Approach to Data Protection Legislation

The EU Directive³²⁵ is a significant development in the protection of privacy and personal information. As well as exemplifying a certain standard of protection, it has implications for Canada's domestic protection of data.

Before proceeding further it will be useful to discuss the general European approach to data protection and to contrast this with the approach of the United States and Canada. European data-protection legislation is highly regulatory and comprehensive in its coverage. This approach is a product of the European public-law orientation, which sees European countries enshrine fundamental rights (including the right to privacy) in broad legislation.³²⁶ In general, European states have adopted either a registration or licensing regime for data protection that applies to both the public and private sectors. In a registration regime, a public or private sector institution which collects or uses personal information must register with a central data protection registrar. A licensing scheme is similar but more stringent. It requires the institution to obtain a licence from the central authority *before* beginning to process personal information. The first wave of European countries to pass data protection legislation adopted licensing systems; the European countries which passed legislation more recently have adopted registration systems. France's

³²⁰ Signed 1966, Annex to G.A. Res. 2200A, 21 U.N. GAOR, Supp (No. 16) 52, U.N. Doc. A/6316, (1966). This Covenant came into force in Canada on August 19, 1976.

³²¹ For the text of the full text of the OECD Guidelines, see for example James Michael, *Privacy and Human Rights* (Paris: UNESCO Publishing, 1994) at 139ff.

³²² *Privacy Commissioner of Canada, Annual Report 1984-85* (Ottawa: Supply and Services Canada, 1985) at 11.

³²³ For further discussion of the OECD guidelines, see the discussion in Part I of this study under the heading The Nature of Privacy and Informational Privacy Issues.

³²⁴ See s. 19 of the OECD guidelines.

³²⁵ *Directive 95/46/EC on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data*, OJ L 281/31 of Nov. 23, 1995.

³²⁶ James Maxeiner, "Business Information and Personal Data: Some Common-Law Observations About the EU Draft Data Protection Directive" (1995) 80 *Iowa Law Review* 619 at 627.

Law of 6 January 1978 on Informatics, Data Banks and Freedoms provides an example of the licensing model, while the United Kingdom's *Data Protection Act*, 1984 provides an example of the registration model.³²⁷

In contrast to the European approach, many non-European countries have adopted a sectoral approach to privacy protection in the private sector. The United States, like Canada, uses the sectoral approach. At the federal and state levels, statutes protect personal information in such areas as credit reporting, electronic funds transfer and the confidentiality of information relating to individuals subscribing to cable television and renting videos.³²⁸ However, there is no comprehensive private-sector privacy legislation in the U.S., nor is there any independent agency responsible for monitoring or overseeing privacy or data-protection rights.³²⁹ Observers have noted that the American approach towards privacy protection appears to be rooted in principles of private rights and libertarian governance.³³⁰ American legislators are reluctant to regulate the private sector without a demonstrated need and focus more on governmental excess than private-sector excess.³³¹ For example, the Clinton administration has refused to develop legislation to protect privacy on the Internet, calling on the private sector to develop and implement privacy codes.³³²

Development of the EU Directive

Council of Europe Convention

One year after the OECD Guidelines were issued, the Council of Europe promulgated the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*³³³ (the “**Convention**”), which took effect in 1985. The Convention requires signatories to implement domestic legislation which gives effect to the Convention's data protection principles. The Preamble to the Convention acknowledges the increasing transborder flow of automatically processed personal information, the desirability of extending safeguards to protect individuals’

³²⁷ For some discussion of the French law, see for example: David H. Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill: University of North Carolina Press, 1989) at 165ff.

³²⁸ Ian Lawson, *Privacy and the Information Highway: Regulatory Options for Canada* (Industry Canada: 1996), available at <http://strategis.ic.gc.ca/SSG/ca00265e.html>.

³²⁹ In 1977, the U.S. Privacy Protection Study Commission expressly decided against establishing an omnibus privacy statute to regulate the flow of personal information for various reasons. The Commission cited the importance of the free flow of information and the difficulty in drafting a statute that would cover all aspects of information collection and use. See: Joseph Rosenbaum, “The European Commission's Draft Directive on Data Protection” (1992) 33 *Jurimetrics Journal of Law, Science and Technology* 1 at 3-4.

³³⁰ Joel Reidenberg, “Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms” (1993) 6 *Harvard Journal of Law. & Technology* 287 at 302.

³³¹ Barbara Wellbery, “An Overview of Information Privacy in the United States and European Union” in *Privacy in Electronic Commerce: A Compendium of Essays on the Use of Information*, ed. by L. Fischer and R. Bennett (Washington: American Bankers Association, 1997) 69 at 75.

³³² U.S. observers have argued that since the Internet, electronic commerce and other media are rapidly evolving, any data-protection legislation would soon be outdated and might well hamper the development of these media. See: Wellbery, *supra*, note 331.

³³³ Jan. 28, 1981, Europ. T.S. No. 108.

right to privacy, and the need to “reconcile the fundamental values of the respect for privacy and the free flow of information between peoples.”

The Convention is similar to the OECD guidelines in content, but whereas the guidelines place more emphasis on the free flow of information, the Convention stresses individual privacy rights to a greater extent. The purpose of the Convention, as set out in Article 1, is to secure for every individual “respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him.” Like the Guidelines, the Convention applies to automatic processing of personal data in both the public and private sectors. “Personal data undergoing automatic processing shall be:

- (a) obtained and processed fairly and lawfully;
- (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- (c) adequate, relevant and not excessive in relation to the purposes for which they are stored;
- (d) accurate and, where necessary, kept up to date;
- (e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.”³³⁴

The Convention also contains provisions dealing with data security, sanctions and remedies, and sensitive personal data. Of particular interest is Article 12, which entitles a Party to the Convention to prohibit transborder flows to a third party whose privacy protection does not provide *equivalent* protection.

Draft of EU Directive

Although the Convention is legally binding upon its Members and requires signatories to enact conforming national laws, not all European countries have ratified the Convention. Moreover, the Convention, like the Guidelines, permits broad variances among national regimes and thus uneven application. Some countries, for example, have created special protection for sensitive data pursuant to Article 6, while others have not.³³⁵ The European Commission was concerned that transborder data transfers would be impaired by the diversity in national data-protection laws, which, in turn, would adversely affect the health of the Common Market and the development of an efficient information structure.³³⁶ Thus, the EU Directive reflects the

³³⁴ *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, Jan. 28, 1981, Europ. T.S. No. 108, Article 5.

³³⁵ Paul Schwartz, “European Data Protection Law and Restrictions on International Data Flows” (1995) 80 *Iowa Law Review* 471 at 478.

³³⁶ Lawson, *supra*, note 328.

European Union's guiding principle of consistency amongst member states. The Union will often err on the side of increased regulation to obtain consistency at the cost of efficiency. In this regard, the Union is not necessarily a federalist model which should be used uncritically.

In July of 1990, the Commission published a draft *Council Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data* (the "**Draft Directive**")³³⁷ with the objective of harmonizing privacy protection legislation of Member States in order to facilitate the free flow of personal data within the European Union. The Draft Directive was more detailed and broader in scope than the Convention; it was, according to one author, part of a program by members of the European Union to go beyond the creation of an economic and monetary union to form a political union as embodied in the Treaty on European Union.³³⁸ The Draft Directive held greater promise of harmonizing Europe's data protection laws than did the Convention since, unlike the Convention, which was only binding on Member States to the extent it had been implemented in their domestic laws, a directive could be relied upon by both citizens and data protection commissioners if a Member nation either failed to implement conforming national data protection laws by a certain date or failed to implement the directive completely.³³⁹

Member States were to enact legislation implementing the Draft Directive by January 1, 1993, but the Commission was obliged to re-draft the proposed directive because of numerous critical comments. The major issue of contention with the Draft Directive related to the provision prohibiting the transfer of data to third countries without an "adequate" level of data protection. It had been hoped that the draft proposal would clarify the ambiguous clause in the Convention which required "equivalent" data protection laws in recipient countries. Not only did the Draft Directive fail to provide any guidance on this matter, but it further complicated the issue by apparently setting up two different levels of protection: an "equivalent" standard of protection was required for transmissions of personal data among Member States while transmissions to non-Member States required an "adequate" level.³⁴⁰

The Draft Directive was also criticized by the United Kingdom, which felt that the directive's requirements went too far beyond its own data protection legislation and that it would impose unnecessary burdens on business. The U.K. government was of the opinion that the Convention provided sufficient legal certainty.³⁴¹ Other countries, such as Germany, were concerned that the Draft Directive was not as comprehensive as their own data protection regimes and would consequently weaken national data protection.³⁴² Other criticism levelled against the Draft Directive included the concern that the amount of direct mail would necessarily increase because

³³⁷ COM (92) 314 final-SYN 287 Brussels, 13 Sept. 1990: (1990) O.J. C277/3.

³³⁸ Fred Cate, "The EU Data Protection Directive, Information Privacy, and the Public Interest" (1995) 80 *Iowa Law Review* 431 at 432.

³³⁹ Schwartz, *supra*, note 335 at 481-482.

³⁴⁰ See Olga Estadella-Yuste, "The Draft Directive of the European Community Regarding the Protection of Personal Data" (1992) 41 *International and Comparative Law Quarterly* 170 at 174-179.

³⁴¹ Fiona Carlin, "The Data Protection Directive: The Introduction of Common Privacy Standards" (1996) 21 *European Law Review* 65 at 65.

³⁴² See Ian Lloyd, "An Outline of the European Data Protection Directive" (1996) 1 *Journal of Information, Law and Technology*, available at <http://eli.warwick.ac.uk/elj/jilt/dp/intros/>.

the directive made it harder to target potential customers. Moreover, it was felt that the Draft Directive would require impractical security requirements and would adversely affect automated decision-making systems.³⁴³ The Draft Directive was also viewed by some critics as a non-tariff barrier to trade or, put more bluntly, a European attack on the profitable U.S. information and programming industries. Privacy experts, on the other hand, were of the opinion that the Draft Directive would put pressure on the U.S. to enhance its privacy-protection measures.³⁴⁴

Harmonization of Data Protection Laws throughout the European Union

There were a number of obstacles to getting the Directive approved by Member States. Although most countries already had specific privacy legislation in place, rather than facilitating the task of drafting the Directive, this proved to be a major handicap since most Member States wanted to preserve their own, familiar rules. Consequently, the drafting of the Directive turned out to be largely an exercise in combining the legislation of Member States, with the range and the content of the Directive determined by existing national laws. Some compromises were required because of key differences in domestic data-protection legislation. For example, the British and Dutch data protection laws encouraged the private sector to draw up their own codes of conduct, but such an approach was foreign to German and French laws.³⁴⁵ National approaches to the processing of certain categories of highly sensitive data and the degree to which the media were exempted from processing personal data also varied. The attempt to compromise and combine these existing national laws created the risk of a lower level of data protection.³⁴⁶ By way of example, in order to appease the objections of the United Kingdom, whose legislation did not apply to manual records, a provision was included in the amended Directive which allowed a 12-year grace period before the processing of data already held in manual files had to be brought into conformity with the Directive.³⁴⁷ The European Commission's objective to regulate the processing of all personal data in the Union also ran into roadblocks in those areas which countries considered to fall within their exclusive jurisdiction. The French and British governments insisted that the processing of personal data by police be exempt from the provisions of the Directive. As a result, paragraph 13 of the *Recitals* to the Directive acknowledges that public safety, defence, State security and the activities of the State in the area of criminal laws falls outside the scope of Community law. The Commission was also forced to compromise by including a provision in the non-binding *Recitals* that the Directive *should* apply

³⁴³ Rosenbaum, *supra*, note 329 at 5.

³⁴⁴ Estadella-Yuste, *supra*, note 340 at 440-441.

³⁴⁵ For a more detailed discussion, see Spiros Simitis, "From the Market to the Polis: The EU Directive on the Protection of Personal Data" (1995) 80 *Iowa Law Review* 445 at 449-450.

³⁴⁶ In a conference held in July of 1996, well after the EU Directive was adopted by its members, academics from Germany, Austria, Norway and Holland voiced their belief that the Directive threatened to reduce the level of data protection provided by their national laws. See A. Wiebe, "Harmonization of Data Protection Law in Europe" (Conference Report) (1996) 3 *The Journal of Information, Law and Technology*, available at <http://ltc.law.warwick.ac.uk/jilt/confs/3dp/default.htm>.

³⁴⁷ Carlin, *supra*, note 341 at 65. It should be noted, however, that the U.K. government is in the process of amending its data protection act and plans on extending the application of the law to certain manual files as well.

to the processing of sound and audio data. It was felt by some members that any regulation of personal data gathered by means of audio-visual technology would interfere with police work.³⁴⁸

Overview of EU Directive

The final version of the EU Directive was adopted on October 24, 1995. European Union member states are required to give effect to the provisions of the EU Directive by October 24, 1998. The dual objectives of the EU Directive are to protect individuals with respect to the processing of their personal data and to ensure a free flow of personal data between Member States through the harmonization of national data protection laws. The EU Directive applies to all processing of personal data by automatic means and to some personal data filed in a manual system.³⁴⁹

The EU Directive sets out a number of data quality principles. Member States must ensure that personal data are: processed fairly and lawfully; collected and processed for specified, explicit and legitimate purposes; adequate, relevant and not excessive in relation to the purposes for which they are collected; accurate and kept up-to-date; and kept for no longer than is necessary.³⁵⁰ Moreover, personal data can only be processed if the data subject has unambiguously given his consent, unless one of a number of exceptions applies. These exceptions include certain contractual and legal obligations and the protection or fulfilment of vital or legitimate interests of either the data subject or the data controller.³⁵¹ Barring certain exceptions, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership is prohibited, as is the processing of data concerning an individual's health or sex life.³⁵²

Data subjects are afforded a number of rights under the EU Directive. When personal data relating to an individual are collected, that person must be informed of the controller's identity, the purposes for which the data are collected and the recipients of the data. Moreover, the controller must inform the data subject of his right to access and rectify the data concerning him. If the data are not obtained directly from the data subject, the controller is still under the obligation to provide him with the same information unless this would prove impossible or would involve a disproportionate effort. In such a case, Member States would have to provide appropriate safeguards.³⁵³ An individual also has the right to object to processing for the purposes of direct marketing³⁵⁴ and the right not to be subject to a decision based solely on automated processing of data if such a decision adversely affects him.³⁵⁵ The EU Directive further provides that individuals have the right to a judicial remedy for any breach of the rights

³⁴⁸ Simitis, *supra*, note 345 at 454.

³⁴⁹ EU Directive, *supra*, note 325, Article 1.

³⁵⁰ *Ibid.*, Article 6.

³⁵¹ *Ibid.*, Article 7.

³⁵² *Ibid.*, Article 8.

³⁵³ *Ibid.*, Articles 10 and 11.

³⁵⁴ *Ibid.*, Article 14.

³⁵⁵ *Ibid.*, Article 15. Automated decisions may be made, however, if suitable measures are in place to safeguard the individual's legitimate interests.

guaranteed in national data protection laws. An individual is also entitled to receive compensation for any damage suffered as a result of an unlawful processing operation or of any act incompatible with national provisions.³⁵⁶

An independent supervisory authority, charged with the task of monitoring and enforcing the application of the EU Directive, must be appointed by each Member State. The supervisory authority is to have investigative powers, powers of intervention and the power to engage in legal proceedings for violations of national data protection legislation adopted pursuant to the EU Directive.³⁵⁷ Data controllers must notify the supervisory authority before they are entitled to process personal data. Information to be supplied during notification includes the purpose of the processing, the recipients to whom the data might be disclosed, and proposed transfers to third countries. The EU Directive does allow Member States to simplify the notification procedures or exempt some data controllers from notification, depending upon whether the processing of the data in question is likely to adversely affect the rights of the data subject.³⁵⁸ The national supervisory authority is also charged with the task of encouraging trade associations and other bodies to draw up codes of conduct and submit them for approval.³⁵⁹

The EU Directive envisages a free flow of data between Member States. With respect to transfers of personal data to a non-member state, the Directive stipulates that these transfers are only permitted if there is an adequate level of protection in that third country. The adequacy of the level of protection provided by a third country is to be assessed in light of all the circumstances surrounding a data transfer operation, with particular consideration given to the nature of the data, the purpose and duration of the proposed processing operation, the country of origin and the country of final destination, the rules of law, both general and sectoral, in force in the third country, and the professional rules and security measures which are complied with in that country.³⁶⁰ Transfer of data to a third country without adequate protection may still take place on condition that:

- the data subject has given his unambiguous consent to the proposed transfer;
- the transfer is necessary for the performance of a contract between the data subject and controller or a contract concluded between the controller and a third party in the interest of the data subject;
- the transfer is required for important public interest grounds or to protect the vital interests of the data subject; or

³⁵⁶ EU Directive, *supra*, note 325, Articles 22 and 23.

³⁵⁷ *Ibid.*, Article 28.

³⁵⁸ *Ibid.*, Articles 18 and 19.

³⁵⁹ *Ibid.*, Article 27.

³⁶⁰ *Ibid.*, Article 25.

- the transfer is made from a register which is open to the public in general or to anyone with a legitimate interest.³⁶¹

“Adequate” Protection and Transfer to Third Countries under the EU Directive

“Adequate” Protection and Legislation in Third Countries

The EU Directive’s restriction on transborder transfers of personal data to countries which do not maintain an adequate level of protection has led to considerable debate about what constitutes “adequate” protection. It has been suggested that privacy protection legislation in Canada and the United States is unlikely to meet the EU Directive’s adequacy criterion because of these two countries’ inadequate notification and remedial procedures. Moreover, the EU Directive’s registration and licensing system is completely foreign to Canada and the United States.³⁶² On the other hand, the U.K. Home Office released a paper in 1996 in which it was opined that “the number of cases in which transfers have to be prohibited because of the inadequacy of data protection in third countries is likely to be small.”³⁶³

The usefulness of the exceptions provided in Article 26, which allow third-country transfers notwithstanding inadequate protection, has also raised some concerns. Many experts feel that only legislation offers data subjects sufficient protection in third-country data transfers and that contractual protection may be ineffective.³⁶⁴ (For a contrary view, see the discussion below on contractual protection.³⁶⁵) It should also be noted that contractual provisions between a data controller and a third party might be ineffective in common-law jurisdictions because of the common-law doctrine of privity of contract. Moreover, it is uncertain what loss the data subject would face which would give rise to a cause of action for damages.

The Working Party on the Protection of Individuals with regard to the Processing of Personal Data (the **“Working Party”**), set up under Article 29 of the EU Directive, released a paper in June 1997 which discussed the issue of “adequate” protection.³⁶⁶ Although the Working Party paper does not provide a definitive approach to this issue, it offers some insight into the Commission’s initial views. The paper notes that while Article 25 envisages a case-by-case approach it is not realistic to examine every case in detail, given the huge number of data transfers that occur on a daily basis. Two mechanisms to rationalize the decision-making process are put forward.

³⁶¹ *Ibid.*, Article 26.

³⁶² A. Perey and H. Janisch, “International Restrictions on the Exchange of Information: Privacy, Transborder Data Flows and Trade in Services” from *Privacy in Financial Services: Striking a Balance between Privacy Rights and Profits* (Toronto: The Canadian Institute, 1994).

³⁶³ U.K. Home Office, *Consultation Paper on the EC Data Protection Directive (95/46/EC)* (March 1996) at chapter 7.1, available at http://www.open.gov.uk.home_off/ccpd/dataprot.htm.

³⁶⁴ Schwartz, *supra*, note 335 at 486.

³⁶⁵ See the discussion below under the heading “Adequate” Protection and Contractual Privacy Provisions.

³⁶⁶ European Commission Directorate General, *First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy: Discussion Document Adopted by the Working Party on June 26, 1997*, available at <http://www.open.gov.uk/dpr/d5020en2.htm>.

First, the paper suggests that officials might develop a “white list” of third countries which could be assumed to offer adequate protection. To be consistent with Article 25, it would be necessary to ground the decision to include a particular country on the “white list” on the basis of individual cases. Once several representative cases of data transfer to a particular country had been considered, and it was determined that adequate protection had been provided, the country in question could be “white listed.” A “partial listing” is a variant of this approach. A country might be “partially listed” if it did not offer uniform protection in all sectors (e.g., if it had protection for the public sector but not the private-sector protection), if it had specific laws for certain industries but not all industries, or if provinces or states within a federal system provided different levels of protection. Particularly if industry codes are legislatively mandated, it would seem unlikely that they would not satisfy European Union requirements.

Second, transfers of information to third countries not on the “white list” could be allowed, depending upon the category of the information being sent. By way of example, transfers involving sensitive categories of data or transfers which carry the risk of financial loss or risk to personal safety would require higher third-country protection than other forms of data.

The paper states that an analysis of “adequate” protection in a given country must consider two key elements – the content of the applicable rules and the means for ensuring their effective application. With respect to the content of applicable rules, the basic principles to be included in any privacy protection scheme consist of the following: the purpose limitation principle; the data quality and proportionality principle; the transparency principle; the security principle; the rights of access, rectification and opposition; and restrictions on onward transfer to other countries. With respect to the means for ensuring the application of the rules, the paper notes that although there is widespread support in Europe that data protection principles should be embodied in law, what is essential is that the protection system: deliver a good level of compliance with the rules; provide support and help to individual data subjects; and provide appropriate remedies to injured parties upon breach of the rules.

There have been a few cases in which European countries, acting under their own national laws, have restricted transborder transfers of data. In 1990, for example, the British Data Protection Registrar prevented the sale of a British mailing list to an American direct-mail organization.³⁶⁷ In another case, France prohibited a French subsidiary of an Italian parent from transferring data to Italy because Italy did not have sufficient data protection legislation in place.³⁶⁸ Although these cases are rather dated, they do make it clear that governments and businesses cannot afford to take the possibility of data transfer restrictions lightly. On the other hand, the “adequacy” criterion of the EU Directive does not really impose any new burdens on third countries since many European countries have already had in place for some time national laws which regulate transborder data transfers, most of which require “equivalent” protection.³⁶⁹

³⁶⁷ U.K. Office of the Data Protection Registrar, *Seventh Annual Report* (1990) at 33-34, cited in Cate, *supra*, note 338 at 438.

³⁶⁸ Law No. 78-17 of Jan. 6, 1978, concerning data processing, records, and freedom, cited in Cate, *supra*, note 338 at 438.

³⁶⁹ See Schwartz, *supra*, note 335 at 474-476.

Whether existing Canadian and American data protection schemes would satisfy these two requirements is debatable, but what is certain is that data transfer restrictions to these two countries would have a negative impact on the American, Canadian, and global economies. Information services and products are said to be either the first or second largest sector of the U.S. economy, accounting for between 10 per cent and 12 per cent of America's Gross Domestic Product. Canada is probably comparable and, if not, we would want to ensure it could be. It is estimated that between one-half and two-thirds of U.S. workers are employed in information-based jobs.³⁷⁰ An Information Infrastructure Task Force, under the Clinton Administration, highlighted the significance of information: "Information is one of the nation's most critical economic resources. In an era of global markets and global competition, the technologies to create, manipulate, manage and use information are of strategic importance to the United States."³⁷¹

"Adequate" Protection and Contractual Privacy Provisions

Where the laws of a proposed recipient country do not meet the standard for "adequate" protection set out in Article 25 of the EU Directive, it may be possible for the transfer to proceed nonetheless, in reliance on an exemption from the restrictions on transfer based on contractual provisions. In particular, Article 26 states that a transfer may proceed without "adequate" legislative protection if the data controller ensures privacy protection through appropriate contractual clauses. A similar concept existed under the earlier European Convention; in fact, the Council of Europe published a model international contract for the protection of privacy under the Convention.³⁷² The German RailwayCard case provides an example in which contractual protection of privacy was used to permit the transfer of personal information between German and American branches of Citibank.³⁷³

The RailwayCard is a card used by German rail travellers to obtain discounts on their train tickets. In 1994, the German railway corporation entered an agreement with the German subsidiary of Citibank (a U.S.-based bank) that would see the RailwayCard offered with a combined Visa credit card. Information about card subscribers would be transferred to a Citibank subsidiary located in South Dakota and Nevada, where the cards would be produced. The plan caused considerable public debate, particularly since people who initially wanted the

³⁷⁰ Cate, *supra*, note 338 at 439-440.

³⁷¹ *Ibid.*, at 439-440, quoting from *Information Infrastructure Task Force, National Information Infrastructure Agenda for Action 5* (1990).

³⁷² Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows with Explanatory Memorandum* (Strasbourg: Council of Europe, November 1992). Extracts from the Model Contract are reproduced in *Sourcebook on Business and Global Data Protection* (Hackensack, N.J.: Privacy and American Business, 1996) at 245ff.

³⁷³ The discussion of the RailwayCard case draws on material provided in article by the Deputy Data Protection Commissioner of Berlin, Germany: Alexander Dix, "The German RailwayCard: A Model Contractual Solution of the 'Adequate Level of Protection' Issue" in *Privacy Beyond Borders: The 18th International Privacy and Data Protection Conference* (Ottawa: September 1996).

RailwayCard were given no choice but to accept the combined Visa card.³⁷⁴ The public feared that German railway monopoly had sold the data of railway customers to a U.S. bank which was likely to use such data for a variety of direct marketing purposes.³⁷⁵ The Berlin Data Protection Commissioner argued that while Articles 25 and 26 of the EU Directive had not yet been incorporated into German legislation, no data transfer to the U.S. should take place unless the requirements of these articles were met. The result was a contractual agreement between the German and U.S. subsidiaries of Citibank involved in the RailwayCard program.

The contract contains a variety of provisions intended to protect the privacy of personal information transferred to the U.S.³⁷⁶ The parties agreed to apply the German data protection law in the handling of cardholder data. The parties agreed not to transfer personal information to third parties for marketing purposes, with two exceptions.³⁷⁷ The U.S. subsidiary agreed to appoint data protection supervisors and accept on-site audits by the Berlin data protection commissioner, or a U.S. auditing firm acting on behalf of the Berlin commissioner. (In fact, U.S. and German bank regulators entered an agreement on the auditing of this account data.) Perhaps most significantly, the U.S. subsidiary agreed that German residents would have the same data rights against the U.S. subsidiary as they would have under German law. Cardholders would have rights of access to and correction of personal information, and the right to bring an action for compensation under the strict liability rules of the German legislation. The agreement may be enforced by cardholders in the German courts; apparently, German law does not raise the same privacy barrier to enforcement that could arise in a common law jurisdiction.³⁷⁸

In a recent article, the Berlin deputy commissioner contended that this contractual solution met the requirements of Articles 25 and 26 of the EU Directive. However, he argued that this approach should not serve as a replacement for legislation protecting privacy rights in the United States and other non-European jurisdictions. Here, he contended that the wording of the EU Directive itself suggests that the exceptions set out in Article 25 to the principle of "adequate" protection are intended as exceptions rather than the norm. "Arguing in favour of standard contractual clauses as a model solution for all trans-border data flows from Europe to third countries would...reverse the relation between the principle and the derogation under European law."³⁷⁹ He also noted that the RailwayCard case involved unusual circumstances, such as the involvement of bank regulators and the receptivity of Citibank to a contractual solution. Finally, contractual arrangements could not replace the need for a central oversight mechanism in foreign jurisdictions such as Canada and the United States. The approach of creating special audit rights by contract would lead to a variety of foreign authorities applying different standards within the jurisdictions.

³⁷⁴ Ultimately, the RailwayCard was offered with the Visa card as an option. The large majority of RailwayCard holders chose the non-Visa version of the card.

³⁷⁵ Dix, *supra*, note 373 at 2.

³⁷⁶ *Ibid.*, at 4-5.

³⁷⁷ First, personal information about Visa card use could be transferred to other Citibank subsidiaries for the marketing of financial services. Second, personal information about users of the "plain" version of the RailwayCard could be transferred solely for the purpose of marketing the Visa version of the RailwayCard.

³⁷⁸ Dix, *supra*, note 373 at 4-5.

³⁷⁹ Dix, *supra*, note 373 at 6.

However, in the case of data transfers to federally-regulated Canadian financial institutions, the unusual circumstances of the RailwayCard case are likely to exist. Regulated financial institutions are generally large and sophisticated; in addition, the Office of the Superintendent of Financial Institutions in Canada might be willing to cooperate to ensure that important data transfers took place. As a result, it is possible that the RailwayCard case could provide a workable model that would permit transfers between European jurisdictions and Canadian financial institutions despite Article 25 of the EU Directive.

Based on the foregoing, it appears that it may be premature to enact any particular privacy scheme with a view to compliance with European standards. First, it is not clear what is required for compliance. Second, there is very little experience on which to take guidance as to compliance. Third, the German RailwayCard case suggests that it may be possible to accomplish at least some transborder data transfers based on contractual provisions rather than legislation in the third party jurisdiction. While it might be too cumbersome for general use, no real experience exists indicating that the EU Directive creates problems now. We also do not know whether the existing self-regulatory, sectoral approach will be “adequate” for European Union purposes or not. A wait and see approach would seem to be the appropriate one at this stage.

Privacy Legislation in the United Kingdom

The *Data Protection Act, 1984*³⁸⁰ received Royal Assent in July of 1984 and was implemented in stages, coming into full force in November of 1987. The U.K. Act was passed after lobbying efforts by members of private industry who feared that the United Kingdom would be excluded from European transborder data transfers.³⁸¹ The Act sets forth a registration model of data protection, in which any person who wishes to process automatic data must register with the Data Protection Registrar. Although the Act’s enforcement provisions and individual remedies are laudable, its strict registration requirements appear to have created bureaucratic obstacles, not only for data users but also for individuals wishing to access their personal information.

Overview of the *Data Protection Act 1984*

The *Data Protection Act 1984* largely regulates the use of automatically processed information by “data users.” The Act applies to a data user if that the user controls the contents and use of data which are held in a form that can be automatically processed³⁸² and which relate to a living individual who can be identified from that information.³⁸³

³⁸⁰ *Data Protection Act 1984*, c. 35.

³⁸¹ See Tom Onyshko, “Access to personal information: British and Canadian Legislative approaches” (1989) 18 *Manitoba Law Journal* 213 at 236-237.

³⁸² The Act does not regulate information contained in manual records.

³⁸³ See s. 1 of the *Data Protection Act 1984* for definitions of “data user,” “data subject,” “data” and “personal data.” Expressions of opinion about an individual qualify as personal data. The Act outlines certain exemptions to registration by data users. Personal data held by an individual and concerned only with the management of his personal, family or household affairs are exempt (s. 33), as are data involving remuneration or pensions in respect of employment and certain sales transactions (s. 32).

A data user is not entitled to hold personal data about an individual until the user has registered with the Data Protection Registrar; contravention of this requirement is a criminal offence.³⁸⁴ Upon registering, the data user must provide, among other things, a description of: the personal data to be held and the purposes for which such data will be held or used; the source from which the data will be obtained; any person to whom the data may be disclosed; and any countries outside of the United Kingdom to which the data may be directly or indirectly transferred.³⁸⁵ If, at a later date, the data user wishes to disclose the data to someone not on the register entry or wishes to collect data for some other purpose, he must apply to the Registrar to make the necessary alterations.³⁸⁶ Failure to do so is also a criminal offence.

A data user is under a duty to adhere to the Act's eight Data Protection Principles, which are largely based upon the Council of Europe Convention principles and which regulate the collection, storage, processing, quality and use of the data and the rights of the data subject. Although a breach of one of the data protection principles is not *per se* a criminal offence, the Data Protection Registrar may take action to de-register the data user if he is of the opinion that the contravention has caused or is likely to cause any person damage or distress.³⁸⁷

The Act sets out certain rights for data subjects. An individual may make a written request (accompanied by a fee) to any data user for access to the individual's own data. The data user then must supply the individual with a copy of the information.³⁸⁸ Separate requests must be made in the case of a data user who has separate entries in the register in respect of data held for different purposes. The Act also establishes a civil action for individuals harmed by misuse of personal information. An individual is entitled to compensation for any damage or distress suffered as a result of the inaccuracy, loss, unauthorized destruction or unauthorized disclosure of data held by a data user.³⁸⁹ A court also may, upon application and subject to certain conditions, order the rectification or erasure of any data held by a data user.³⁹⁰

The Act creates the Data Protection Registrar who, in addition to maintaining a register of data users, is charged with the duty of promoting the observance of the data protection principles. To this effect, the Registrar has the power to prosecute any data user who fails to register or knowingly or recklessly acts outside the scope of a register entry. The Registrar also may refuse an application for registration by a data user where he feels that the applicant is likely to contravene any of the data protection principles.³⁹¹ If the Registrar believes that a registered data user has breached any of these principles, he may serve this person with an "enforcement notice," requiring the data user to rectify the matter,³⁹² or a "de-registration notice," which cancels the data user's registration.³⁹³ The Registrar may serve upon a data user a "transfer prohibition

³⁸⁴ *Data Protection Act 1984, supra*, note 380, s. 5. Note that computer bureaux are also required to register.

³⁸⁵ *Data Protection Act 1984, supra*, note 380, s. 4.

³⁸⁶ *Ibid.*, s. 6.

³⁸⁷ *Ibid.*, s. 11.

³⁸⁸ *Ibid.*, s. 21.

³⁸⁹ *Ibid.*, ss. 22 and 23.

³⁹⁰ *Ibid.*, s. 24.

³⁹¹ *Ibid.*, s. 7(2).

³⁹² *Ibid.*, s. 10.

³⁹³ *Ibid.*, s. 11.

notice,” which can prevent the data user from transferring personal data outside the United Kingdom. In addition, the Registrar has a duty to encourage the production of codes of practice in the private sector. However, unlike New Zealand’s legislation, such private sector codes are not legally enforceable under the U.K. Act.

The implementation of this highly regulatory data protection legislation was a marked departure from the U.K. trend towards government deregulation.³⁹⁴ Although the Act was specifically implemented to satisfy treaty obligations, its universal system of registration came under considerable criticism. One Opposition Committee member referred to the Bill as a “Data Registration Bill” and expressed his concern that the Registrar and his staff would become

little more than recording agents for the many registrations received. Far from exercising some control, the Registrar will find himself bogged down in day-to-day administration. He will be able to supply no data protection safeguards.³⁹⁵

The registration system proved to be less of a debacle than the above comments would suggest, but compliance with and enforcement of the registration system have been less than optimal.³⁹⁶ The 1995 *Annual Report* of the Office of the Data Protection Registrar admitted that registration was a hurdle that had to be jumped: there was clear under-registration and a low rate of renewals.³⁹⁷ The Registrar has recently called for a simplification of the registration system and more exemptions from notification.

Proposed Changes to the Act in Light of the EU Directive

Member States of the EU Directive are required to have national legislation giving effect to the EU Directive by October 24, 1998. Although the *Data Protection Act 1984* and the EU Directive are alike in many respects, there are a number of significant differences which necessitate modification of the Act.³⁹⁸ By way of example, the EU Directive has provisions which place restrictions on fully-automated decision making and which require that data subjects be given the right to object to lawful processing of their data or to their data being used for direct marketing purposes. The EU Directive’s rules with respect to the transfer of personal data outside the European Union also differ from those of the Act.

³⁹⁴ M. Stallworthy, “Data Protection: Regulation in a Deregulatory State” (1990) 11 *Statute Law Review* 130 at 130.

³⁹⁵ P. Snape, *HC Debs*, Standing Committee H, col. 70 (26 April 1983), cited in Stallworthy, *supra*, note 394, at 143.

³⁹⁶ *Ibid.*

³⁹⁷ The Office of the Data Protection Registrar, *Annual Report 1995* at Chapter 4, available at <http://www.open.gov.uk/dpr/chap4.htm>.

³⁹⁸ U.K. Home Office, *Consultation Paper on the EC Data Protection Directive (95/46/EC)* (March 1996), available at http://www.open.gov.uk/home_off/ccpd/dataprot.htm.

The U.K. government was initially inclined to adopt a minimalist attitude and make only the changes needed to ensure that the Act complied with the EU Directive. The Registrar of Data Protection, on the other hand, urged the government to make fundamental changes.³⁹⁹ In particular, the Registrar recommended that the registration process should be “radically simplified by extensive exemption and simplification to remove ‘red tape’ burdens.”⁴⁰⁰ The Registrar’s time and resources should be concentrated on data processing that represented a real risk to data subjects; exemptions from notification should be permitted for those data users whose processing was unlikely to adversely affect the rights of data subjects.⁴⁰¹

In its paper, *Data Protection: the Government’s Proposals*,⁴⁰² the Home Office expresses its desire to avoid placing unnecessary burdens on business and consequently indicates its intention to accept many of the recommendations made by the Registrar. Most significantly, the government intends to implement simplified notification and registration requirements. The revised registration scheme would minimize the detail the controller (i.e., the data user) has to provide, would allow a range of notification methods (including on-line access), and would implement a greatly simplified format, including the use of standard packages. Moreover, certain processing operations would be exempt from notification, such as operations carried out for the purposes of payroll and personnel administration, purchase and sales administration, advertising, marketing and public relations and general administration. Notification requirements would not apply to manual records. Other changes to be implemented in the new legislation include extension of the data protection provisions to some manually processed data and individual entitlement to seek redress in court for breaches of privacy rights.

Privacy Legislation for the Private Sector in Quebec

As discussed earlier in this study, Quebec’s *Act respecting the protection of personal information in the private sector*⁴⁰³ (also known as Bill 68) came into force in January 1994. The Act follows earlier privacy legislation that applied to the public sector,⁴⁰⁴ and fleshes out various privacy provisions for the private sector that are included in the *Civil Code* of the Province.⁴⁰⁵ The Act applies to a wide range of private sector entities, including corporations, sole proprietorships,

³⁹⁹ “The Registrar’s preference would be for a completely new Act of Parliament setting out a seamless law of data protection, declaring that it concerns the privacy of individuals, having the existing eight Data Protection Principles at its heart to determine the rights of individuals and the duties of data controllers, and establishing a flexible administrative and enforcement structure which can be readily adapted to cope with changing technology, its applications and social circumstances.” See: The Office of the Data Protection Registrar, *Consultation Paper on the EC Data Protection Directive (95/46/EC): Response of the Data Protection Registrar* (July 1996), available at <http://www.open.gov.uk/dpr/answer/content.htm>.

⁴⁰⁰ *Ibid.* at <http://www.open.gov.uk/dpr/answer/summary.htm>.

⁴⁰¹ *Ibid.* at <http://www.open.gov.uk/dpr/answer/ans6-7.htm>.

⁴⁰² U.K. Home Office, *Data Protection: the Government’s Proposals* (July 1997), available at <http://www.homeoffice.gov.uk/datap3.htm>.

⁴⁰³ R.S.Q. c. P-39.1. For further discussion of the Act, see Part II under the heading Quebec’s Private Sector Privacy Legislation.

⁴⁰⁴ *An Act respecting Access to documents held by public bodies and the Protection of personal information*, R.S.Q. c. A-2.1.

⁴⁰⁵ See the *Civil Code of Quebec*, articles 35-41.

partnerships, organizations and associations. Various provisions govern the collection, use and transfer of personal information; in addition, the Act also establishes the individual's right to gain access to personal information and request a correction where it appears inaccurate. Special provisions apply to lists of names used for marketing purposes and also to transfers of information about Quebec residents to third parties outside the province. Disputes under the Act are to be resolved by the body responsible for resolving disputes under Quebec's public sector access and privacy statute, the Commission d'accès à l'information.

The Quebec Act provides an example of legislation that is similar to European data protection legislation, without the element of mandatory registration or licensing. As the Quebec commission's counsel and president wrote in a law journal article, Quebec legislators adapted the European approach to the North American context: "Hence, any form of mandatory entry in a central register by the holders of personal information files is absent, with the exception of personal information agents made up almost exclusively of credit [reporting agencies]."⁴⁰⁶ The authors argued that the decision to avoid a general registration system led to the greater acceptance of the legislation in the private sector.

There has been relatively little commentary on the Act and its operation. In one early article, Montreal lawyer Christine Carron warned that Bill 68 could have a negative impact on the business community in Quebec: "The new requirements of the Act will certainly increase the costs of doing business, which leaves one wondering whether employees, consumers, entrepreneurs and the society in general will really be better off."⁴⁰⁷ However, the president of the Commission d'accès à l'information has suggested that the Act does not involve a dramatic departure from previous business practices, because many Quebec businesses already had policies that dealt with privacy matters.⁴⁰⁸ Materials available from the Commission itself suggest that it has not been overwhelmed by private sector privacy complaints. For example in 1995-96 the Commission received 151 complaints respecting the private sector, and in 1996-97, 224 such complaints.⁴⁰⁹ We are not aware of any study that has assessed the costs of compliance with the Act.

Privacy Legislation in New Zealand

New Zealand applied data protection principles to both the public and private sectors through the *Privacy Act 1993*. The Act is the latest in a series of New Zealand statutes dealing with privacy

⁴⁰⁶ Paul-André Comeau and André Ouimet, "Freedom of Information and Privacy: Quebec's Innovative Role in North America" (1995) 80 *Iowa Law Review* 651 at 668.

⁴⁰⁷ See: Christine A. Carron, "Overview of the Quebec Act Respecting Personal Information in the Private Sector" in *I've Got A Secret: The Duty of Confidentiality in the Private Sector* (Toronto: Canadian Bar Association - Ontario, March 1994) at 14.

⁴⁰⁸ The president made these comments several months before the Act came into force: Paul-André Comeau, "The Protection of Personal Information in the Private Sector: An Important Step Forward by Quebec's National Assembly," Paper presented to the 6th Annual Conference of Privacy, Laws and Business in Oxford, U.K., 28 June 1993 at 13.

⁴⁰⁹ See: Commission d'accès à l'information du Québec, *Vie privée et transparence administrative au tournant du siècle* (June 1997) at 1.3.3 and Graphique 10, available at <http://www.cai.gouv.qc.ca/sunset1.htm>.

issues⁴¹⁰ and has several interesting features, which include the enforceable status given to approved Codes of Practice and special provisions that regulate authorized data matching activities.

Overview of New Zealand's *Privacy Act 1993*

At the core of the New Zealand *Privacy Act* are 12 "Information Privacy Principles" which deal with the collection, storage, quality and use of personal information, as well as the data subject's rights to access and rectify this information.⁴¹¹ The principles apply to information held by every "agency,"⁴¹² defined as "any person or body of persons, whether corporate or unincorporated, and whether in the public sector or the private sector."⁴¹³ Each agency must have at least one designated privacy officer, whose role is to encourage compliance with the privacy principles, answer requests for personal information, and work with the Privacy Commissioner in the investigation of complaints.⁴¹⁴

Although the Information Privacy Principles do not differ substantially from the principles outlined in most privacy codes and laws, there are some differences worth noting. Principle 2 of the Act requires an agency to collect information directly from the individual concerned, barring a certain number of exceptions. Principle 12 adds a new element to the Act which is not found in Canadian privacy legislation. An agency is not allowed to assign a unique identifier to an individual unless such an assignment is necessary to enable the agency to carry out its functions efficiently. Moreover, the identifier, once assigned by one agency, is not to be used by any other unassociated agency. Since the identifier is intended to be purpose-specific, the government, for example, would not be able to assign one personal number to its citizens for all their dealings with the government.

⁴¹⁰ Legislation enacted in New Zealand in the 1950s and 1970s attempted to provide protection of personal information gathered for the purposes of health, tax, statistics and law enforcement matters. The *Official Information Act*, which came into effect on July 1, 1983, gave individuals the legally enforceable right to access and correct personal information held by government departments and state-owned enterprises. In 1988, the monitoring body established to oversee the operation of the *Official Information Act* tabled a report with the House of Representatives that advocated amendments to the *Official Information Act* to regulate the collection and use of personal information. The Labour government was considering making the necessary legislative changes but lost the general elections before it could implement any amendments. In opposition, the Labour Party continued to emphasize the urgency of privacy protection and in 1991 introduced a Private Member's Bill on privacy. In response to the Private Member's Bill and to public concern about a proposed computer matching program, the government tabled its own legislation. The *Privacy Commissioner Act* was passed on December 18, 1991 to enable the Government to proceed with its data matching program. The *Privacy Act 1993* was then passed in May of 1993. See John Howells, "The *Privacy Act of 1993: A New Zealand Perspective*" (1995) 17 *Comparative Labor Law Journal* 107.

⁴¹¹ *Privacy Act 1993*, s. 6.

⁴¹² *Ibid.*, s. 8.

⁴¹³ *Ibid.*, s. 2. A few exceptions to this rule are listed in this section.

⁴¹⁴ *Privacy Act 1993*, s. 23.

The Act sets out four additional principles, known as the “Public Register Privacy Principles,” that apply to the administration of public registers.⁴¹⁵ Government departments administering public registers are “agencies” under the Act and, as a result, must comply with *both* the Information Privacy Principles and the Public Registry Principles. The four Public Register Privacy Principles are as follows:

Personal information shall be made available from a public register only by search references that are consistent with the manner in which the register is indexed or organized.

Personal information obtained from a public register shall not be re-sorted, or combined with personal information obtained from any other public register, for the purpose of making available for valuable consideration personal information assembled in a form in which that personal information could not be obtained directly from the register.

Personal information in a public register shall not be made available by means of electronic transmission, unless the purpose of the transmission is to make the information available to a member of the public who wishes to search the register.

Personal information shall be made available from a public register for no charge or for no more than a reasonable charge.⁴¹⁶

The New Zealand Act includes special provisions on codes of practice for the public or private sector.⁴¹⁷ A Code of Practice which has been issued by the Privacy Commissioner is an enforceable and legally binding document. It may modify one or more of the Information Privacy Principles by exempting actions or by prescribing standards that are more or less stringent. In addition, it may prescribe how the principles are to be applied. In short, a code will determine how agencies in a particular activity, industry, profession or sector comply with the Information Privacy Principles. Codes of Practice may be initiated either by the Privacy Commissioner or by an “agency” (typically trade associations, professional bodies, or government departments⁴¹⁸). Before the Privacy Commissioner may issue the Code of Practice, the Commissioner must give public notice of the draft code and its relevant details; interested parties may then make submissions on the proposed code to the Privacy Commissioner within a stipulated time frame. A substantial portion of the Code of Practice should deal with the privacy

⁴¹⁵ *Ibid.*, s. 59. The main public registers include the births and deaths register, the register of titles, the companies office registers, electoral rolls, register of drivers licences, motor vehicles, and security interests. See the Second Schedule of the *Privacy Act 1993* for a complete list.

⁴¹⁶ *Privacy Act 1993*, s. 59

⁴¹⁷ For some purposes, the Codes of Practice will have the status of regulations: *Privacy Act 1993*, s. 50.

⁴¹⁸ See Office of the Privacy Commissioner of New Zealand, *Guidance Note on Codes of Practice under Part VI of the Privacy Act*, s. 2.0, available at <http://io.knowledge-basket.co.nz/privacy/guide/cop.htm>.

principles and how compliance with each principle will be achieved. It is also expected that codes will include practical examples.⁴¹⁹

Only three Codes of Practice are currently in effect: the *Health Information Privacy Code 1994*,⁴²⁰ the *Superannuation Schemes Unique Identifier Code 1995* and the *EDS Information Privacy Code 1997*.⁴²¹ All of these codes were initiated by the Commissioner in collaboration with the agencies and industries concerned. The Health Information Code applies to various agencies and kinds of medical information; the code's 12 health information privacy rules essentially mirror the Information Privacy Principles of the Act, with minor modifications to tailor the Act's principles to the health-services context.⁴²² The Superannuation Code was issued at the request of the Association of Superannuation Funds of New Zealand to modify Principle 12 of the Act to permit the sharing of employer-assigned unique identifiers between workplaces and the trustees of workplace-based superannuation schemes.⁴²³ The EDS Code applies to EDS (NZ) Ltd., a private company that processes sensitive information provided by a number of public bodies. The Code prohibits EDS (NZ) Ltd. from transferring any information received from designated agencies outside New Zealand, except with the written consent of the concerned agency and notice to the Privacy Commissioner.⁴²⁴

⁴¹⁹ *Ibid.* at ss. 5 and 6. According to the 1994-95 Annual Report, only two codes of practice were issued during that year. See: Office of the Privacy Commissioner of New Zealand, *Report of the Privacy Commissioner for the Year Ended June 1995* (1995) at s. 3.2, available at <http://io.knowledge-basket.co.nz/privacy/anr>. A more recent discussion paper suggests that only a few Codes of Practice have been issued to date, and all of them have been initiated by the Privacy Commissioner. See: Office of the Privacy Commissioner of New Zealand, *Review of the Privacy Act 1993: Discussion Paper No. 4 – Codes of Practice and Exemptions* (September 1997) at <http://www.knowledge-basket.co.nz/privacy/discpp/discpr4.htm>.

⁴²⁰ The *Health Information Privacy Code 1994* replaced the *Health Information Privacy Code 1993 (Temporary)*. The temporary code issued shortly after the *Privacy Act* came into force without the requisite consultation procedures mandated by the Act. See: Bruce Slane, *Centralised Databases: People, Privacy and Planning* (A paper presented by the Privacy Commissioner to the New Zealand – Australia Health IT Directors Meeting) (February 18, 1998), available at <http://www.knowledge-basket.co.nz/privacy/speeches/itdirect.htm>.

⁴²¹ The *EDS Information Privacy Code 1997* replaced the *GCS Information Privacy Code 1994*. GCS Limited was a state-owned company which processed sensitive information provided by public bodies; however, GCS Limited was privatized and is now owned by EDS (NZ) Limited.

⁴²² For example, Rule 11 of the Code allows for greater disclosure of information than that permitted by Principle 11, though in narrowly-defined areas, and Rule 12 allows certain agencies listed in a schedule to the Code to assign a unique identifier number to an individual, notwithstanding that another listed agency has already assigned the same number.

⁴²³ See: Office of the Privacy Commissioner of New Zealand, *Report of the Privacy Commissioner for the Year Ended June 1995* (1995) at s. 3.2, available at <http://www.knowledge-basket.co.nz/privacy/anr/04repcop.htm>. According to Mr. Blair Stewart of the Office of the Privacy Commissioner of New Zealand, the industry was invited by the Commissioner to produce the Code, it was unable to take on this task and thus the Commissioner was obliged to take charge of the drafting.

⁴²⁴ See: Office of the Privacy Commissioner of New Zealand, *Report of the Privacy Commissioner for the Year Ended June 1995* (1995) at s. 3.2, available at <http://io.knowledge-basket.co.nz/privacy/anr>. See also introduction to *EDS Information Privacy Code 1997*.

The Act also regulates certain information matching programs undertaken by public agencies. Information matching programs are defined as programs that compare personal information records involving 10 or more individuals for the purpose of producing or verifying information about individuals.⁴²⁵ The Act's special provisions apply when specified public agencies seek to undertake information matching programs authorized by other pieces of New Zealand legislation. A short list of "specified" agencies is set out in the Act,⁴²⁶ while a list of "authorized" data matching programs is set out in a schedule.⁴²⁷ (If a public agency conducts an information matching program which does not fall within the "authorized" list and which is otherwise permissible according to the Information Privacy Principles, no special provisions will regulate the program.⁴²⁸) To perform authorized data matching programs, specified agencies must sign agreements that restrict the disclosure of information.⁴²⁹ The specified agency running the authorized matching program may receive only limited access to the other's database; on-line computer transfers of information require the approval of the Privacy Commissioner.⁴³⁰ If a specified agency wishes to take some other adverse action against an individual on the basis of authorized matching program, it must give the individual five days' written notice.⁴³¹ The details of any authorized data matching program must be provided by the specified agencies involved to the Privacy Commissioner. In addition to these special provisions applying to public agencies, the Act states that a Code of Practice may impose controls upon the information matching activities of private sector agencies.⁴³²

The Act is enforced by the Privacy Commissioner, the Proceedings Commissioner and the Complaints Review Tribunal. The duties of the Privacy Commissioner include issuing Codes of Practice, examining any legislation or policy in light of its effect on individual privacy, educating the public on the privacy principles, promoting the privacy principles and handling complaints.⁴³³ An individual may complain to the Privacy Commissioner for any interference with his or her privacy which causes some loss or damage, results in significant humiliation or loss of dignity, or adversely affects the interests of the individual. "Interference" occurs when there is a breach of a principle or a code of practice, or non-compliance with the information matching rules.⁴³⁴ "Interference" also occurs when an agency refuses an individual's access request or request to

⁴²⁵ *Privacy Act 1993*, s. 97.

⁴²⁶ *Ibid.*

⁴²⁷ See the Third Schedule of the *Privacy Act 1993*, which lists provisions authorizing information matching that appear in the *Births and Deaths Registration Act*, *Penal Institutions Act*, *Marriage Act*, *Customs Act*, *Inland Revenue Department Act*, *Immigration Act*, *Education Act* and *Accident Rehabilitation and Compensation Insurance Act*.

⁴²⁸ See Office of the Privacy Commissioner of New Zealand, *Review of the Privacy Act 1993: Discussion Paper No. 7 – Information Matching* (September 1997), available at <http://io.knowledge-basket.co.nz/privacy/discpp/discpr7.htm>, under the heading "The Scheme for Enforcement – What information matching activities ought to be controlled?"

⁴²⁹ *Privacy Act 1993*, s. 99.

⁴³⁰ See s. 3 of the Fourth Schedule of the *Privacy Act 1993*. See also Office of the Privacy Commissioner of New Zealand, *Information Matching: Fact Sheet No. 5* (August 1993), available at <http://io.knowledge-basket.co.nz/privacy/facts/fact5.htm>.

⁴³¹ *Privacy Act 1993*, s. 103.

⁴³² *Ibid.*, s. 46(4)

⁴³³ *Ibid.*, Part III, ss. 12 to 26.

⁴³⁴ *Ibid.*, s. 66(1).

correct personal information, without a valid reason.⁴³⁵ The Privacy Commissioner has power to help settle complaints,⁴³⁶ call compulsory conferences to bring about a settlement,⁴³⁷ and refer complaints to the Proceedings Commissioner if the Privacy Commissioner is unable to resolve the problem.⁴³⁸ The Proceedings Commissioner or the aggrieved individual may, in turn, take the matter before the Complaints Review Tribunal, which has the authority to grant various remedies if it is satisfied on the balance of probabilities that any action of the defendant is an interference with the privacy of an individual. The Complaints Review Tribunal may make a declaration that the action of the defendant is an interference with the privacy of an individual and may order the defendant to refrain from continuing the interference or to perform any specified acts to remedy the interference. The Tribunal may also order any other relief it thinks fit, including damages.⁴³⁹

Rationale for Extending Privacy Protection to the Private Sector

In a recent address to a banking law conference, New Zealand's Privacy Commissioner Bruce Slane discussed the reasons that justified extending privacy protection to the private sector.⁴⁴⁰ Given that a number of state-owned enterprises would pass or had already passed into private ownership, Mr. Slane said that it would be inconsistent to insist that the activities of a particular company be included within the privacy law while it was publicly-owned and yet not covered while privately-owned. Moreover, since the credit, banking and telecommunications industries might contain a mix of publicly and privately owned businesses, the privacy laws should apply to all to ensure a level playing field. Mr. Slane said that it was incorrect to assume that only the public sector required privacy legislation because *only* the state collected information coercively. The reality was that many private-sector companies required personal information before providing their services. Individuals were more concerned about *how* their information was used than who collected or held it. Finally, Mr. Slane argued that sectoral legislation was undesirable because the development of sectoral laws was expensive and time-consuming and would be subject to intensive lobbying which could result in uneven standards.

Mr. Slane noted that the Bankers Association was initially opposed to the application of the Act to the private sector in general and the banks in particular; it was felt that banks were already subject to a number of statutory obligations. In practice, banks have not had any major

⁴³⁵ *Ibid.*, s. 66(2).

⁴³⁶ *Ibid.*, s. 74.

⁴³⁷ *Ibid.*, s. 76.

⁴³⁸ *Ibid.*, s. 77.

⁴³⁹ *Ibid.*, s. 85. The 1994-95 Annual Report notes that of the 827 complaints received within the Commissioner's jurisdiction during the year, 78 per cent were closed without the Commissioner having to give a final opinion. Forty-seven per cent of the complaints dealt with requests for a review of an agency's decision not to make available certain personal information. Most of the other types of complaints were allegations of disclosure of information, especially health information. The Annual Report also noted that 56 per cent of the complaints were levelled against the private sector. See: Office of the Privacy Commissioner of New Zealand, *Report of the Privacy Commissioner for the Year Ended June 1995* (1995) at s. 3.3, available at <http://io.knowledge-basket.co.nz/privacy/anr>.

⁴⁴⁰ Bruce Slane, Privacy Law Issues – Reform Proposals and their Impact on the Financial Industry: Notes for an Address by the Privacy Commissioner for New Zealand to the 14th Annual Banking Law and Practice Conference, May 22, 1997, available at <http://www.knowledge-basket.co.nz/privacy/speeches/banksyd2.htm>.

difficulties in complying with the Act, have not attracted many complaints from customers, and have not sought to implement a code of practice. Mr. Slane also addressed the issue of compliance costs and stated that a voluntary regime of privacy protection, if meaningful, would not likely be less costly. Privacy issues would not disappear just because there was no legislation in place: firms would still have to deal with these issues, and thus there would always be costs involved.

Privacy Act Review

The Privacy Commissioner is currently reviewing the operation of the New Zealand Act to consider whether any amendments are necessary. The Commissioner is fielding comments on such issues as whether new offence provisions should be included in the Act and whether the courts should have jurisdiction in enforcing Information Privacy Principles. The current Act emphasizes civil remedies. Although it is not an offence to breach a principle, if an individual is thereby harmed, the Act can provide a resolution to the problem and may require that the individual be compensated.⁴⁴¹ Another issue under scrutiny concerns compliance costs. It is acknowledged that excessive compliance costs can discourage growth and employment, erode international competitiveness and hinder compliance. At present, the Act imposes no base level of costs, and there are no direct compliance costs in registration or fees. Agencies are responsible for devising their own procedures and forms.⁴⁴² The issue of whether a transborder data flow control is warranted is also being examined.⁴⁴³

Privacy Legislation Developments in Australia

The Australian commonwealth government had considered extending privacy legislation to the private sector, but recently decided against this course of action. Australia partially implemented the OECD guidelines by enacting the *Privacy Act* 1988, which requires commonwealth government departments and agencies to comply with several Information Privacy Principles. The Australian Act does not, however, govern the state government sector and only regulates the private sector in the areas of credit reporting and tax file numbers.

In 1995, a standing committee of the Australian House of Representatives released a paper which unanimously recommended extending the Information Privacy Principles of the Australian Act to

⁴⁴¹ Office of the Privacy Commissioner of New Zealand, *Review of the Privacy Act 1993: Discussion Paper No. 1 – Structure and Scope* (September 1997), available at <http://www.knowledge-basket.co.nz/privacy/discpp/discpr1.htm>.

⁴⁴² Office of the Privacy Commissioner of New Zealand, *Review of the Privacy Act 1993: Discussion Paper No. 9 – Compliance and Administration Costs* (September 1997), available at <http://www.knowledge-basket.co.nz/privacy/discpp/discpp9.htm>.

⁴⁴³ Office of the Privacy Commissioner of New Zealand, *Review of the Privacy Act 1993: Discussion Paper No. 12 – New Privacy Protections* (September 1997), available at <http://www.knowledge-basket.co.nz/privacy/discpp/discpr12.htm>.

the private sector.⁴⁴⁴ The committee felt that a national privacy policy was needed in light of the continuing trend towards privatization and the contracting out of government services. As well, such a privacy policy was needed to address the challenges posed by the information highway. In 1996, the Law Reform Commission recommended that a national legislative scheme be implemented to provide information privacy protection in the public and private sectors.⁴⁴⁵ Later in the year, a discussion paper released by the Attorney General's Department advocated the extension of privacy protection legislation to the private sector.⁴⁴⁶ This paper outlined a co-regulatory approach whereby statutory privacy principles would apply unless an approved Code of Practice, based on the privacy principles, had been implemented. The Codes of Practice could be tailored to meet the needs of particular industries and would thus provide flexible approach for the private sector.

The Australian Financial System Inquiry which reviewed issues facing the financial services industry in Australia issued a report in early March 1997 (the "**Wallis Report**")⁴⁴⁷ The Inquiry made several recommendations for a privacy regime for the financial services industry, based on the assumption that privacy rules for the industry should be the same as those being implemented in the broader economy.⁴⁴⁸ Significantly, the Wallis Report recommended that negative consent arrangements to information sharing should be permitted. A financial institution could obtain consent to information sharing based on the customer's failure to take some action to indicate his or her refusal; however, the institution would be required to provide the customer with a readily available opportunity to refuse.⁴⁴⁹ The Wallis Report concluded that any privacy regulation must strike an appropriate balance between public concerns about privacy of information and the ability of financial institutions to use such information for commercial purposes and to provide financial services more efficiently. Privacy codes should be administered on a national basis, and should apply to all businesses supplying financial services, including non-financial institutions providing financial services.⁴⁵⁰

⁴⁴⁴ House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995).

⁴⁴⁵ Law Reform Commission, *Report of the Review by the Australian Law Reform Commission and the Administrative Review Council of the Federal Freedom of Information Act 1982*, tabled in Parliament on January 24, 1996.

⁴⁴⁶ Attorney General's Department, *Privacy Protection in the Private Sector* (September 1996), available at <http://www.agps.gov.au/customer/agd/clrc/privacy.htm>.

⁴⁴⁷ *Final Report of the Financial System Inquiry* (Australia: March 18, 1997).

⁴⁴⁸ *Ibid.*, at 17.

⁴⁴⁹ *Ibid.*, Recommendation 100, at 66 and 519-521.

⁴⁵⁰ *Ibid.*, Recommendation 101, at 66; 516-517 and 521-523.

Despite these developments, the proposal to extend privacy legislation to the private sector was not implemented. In a press release issued March 21, 1997, the Australian Prime Minister argued that the proposal would impose too great a burden on the private sector: "At a time when all heads of government acknowledge the need to reduce the regulatory burden, proposals for new compulsory regimes would be counterproductive."⁴⁵¹ The Prime Minister also asked premiers of the Australian states not to introduce legislation on this matter in their own jurisdictions. The commonwealth government's change in position was criticized by national and international privacy groups. Privacy International noted that there was "widespread industry and community support for the legislation"⁴⁵² and that the "government's decision goes starkly against the grain of international policy."⁴⁵³

A consultation paper released in August, 1997 by the Privacy Commissioner of Australia attempts to outline a self-regulatory option.⁴⁵⁴ The paper notes that there are differences in opinion as to the desirability of a legislated scheme over a self-regulatory scheme, but businesses invariably favour a scheme which minimizes compliance costs and reduces overlap with other regulations and differences between jurisdictions. Australian trade and businesses also benefit from transborder data flows and so have a concern about the EU Directive. The scheme proposed consists of three components: principles or standards for handling personal information; processes for businesses to sign on to the scheme and for promoting and monitoring compliance with the principles; and mechanisms for handling complaints and providing effective remedies. The paper acknowledges the difficulties in ensuring compliance in a self-regulated regime, and advocates a system wherein businesses will bind themselves to comply with the privacy scheme and provide remedies in the event of a breach of standards. Monitoring would be provided by an independent scheme administrator and an independent body could be put in place to provide an appeal mechanism. The federal government of Australia appears to face similar constitutional constraints to those of the Canadian federal government.

⁴⁵¹ The Rt. Hon. John Howard, Prime Minister's Press Release (March 21, 1997), available at <http://www.efa.org.au/Issues/Privacy/pmpr0321.html>.

⁴⁵² Privacy International, "Looking for Answers on Government's Privacy U-Turn" from *Privacy International Online Privacy Archive* (April 1997), available at http://www.privacy.org/pi/countries/australia/campaign97/coalition_statement_497.html.

⁴⁵³ Privacy International, "Open letter from Privacy International to the Prime Minister of Australia" dated April 16, 1997, available at http://www.privacy.org/pi/countries/australia/campaign97/pi_letter_497.html. See also Tom Dixon, "Voluntary Code Leaves Privacy Exposed," *Australian Privacy Foundation Media Release*, dated August 19, 1997, available at <http://www.efa.org.au/Issues/Privacy/pr0819.html>. Mr. Dixon, Director of the Privacy Foundation, lamented the inadequacy of Australia's privacy laws: "Time is also running out for us to meet the European Union's standards on privacy protection. We only have until October 1998 before Australian industries are excluded from international trade in information. If the Government is serious about assisting Australia's information industries they will establish privacy safeguards that comply with international best practice."

⁴⁵⁴ Privacy Commissioner in Australia, *Information Privacy in Australia: A National Scheme for Fair Information Practices in the Private Sector* (August 1997), available at http://www2.austlii.edu.au/itlaw/national_scheme/national-INFORMAT.html.

Until recently, there had been little privacy legislation in the various Australian states, but new initiatives are underway in New South Wales, Victoria, and Queensland. In New South Wales, proposed privacy legislation would allow for codes of practice to be made by regulation; these codes could be extended to public and private-sector agencies and would be enforceable.⁴⁵⁵ Victoria has considered different regulatory regimes for the protection of privacy, but it is not clear if the state will proceed in light of the Commonwealth's decision to reject private sector legislation.⁴⁵⁶ Queensland is in the process of considering privacy legislation. A discussion paper released by the Queensland Legal, Constitutional and Administrative Review Committee considers several options for greater privacy protection.⁴⁵⁷

⁴⁵⁵ Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland: Issues Paper No. 2* (May 1997), available at http://www.parliament.qld.gov.au/committees/legalrev_issues_paper_2.html.

⁴⁵⁶ *Ibid.*

⁴⁵⁷ *Ibid.* The options considered in the discussion paper consist of the following: A statutory tort could be created to allow individuals to sue for breach of their privacy, but there would be difficulties in properly defining privacy. A privacy commissioner or committee could be established to draft and recommend industry codes of practice and to investigate privacy complaints. The Information Privacy Principles could be implemented administratively, in which case they would apply only to the public sector, or by legislation, in which case they could cover the private sector as well. Privacy protection could take the form of self-regulation by industry codes, but such an option would raise concern that the codes might not be enforced. The discussion paper offers no recommendations, but it does note that a state-by-state approach to privacy standards could be cumbersome, expensive, and detrimental to transborder data transfers.

V. Privacy, Constitutional Jurisdiction and Federal-Provincial Cooperation

Introduction

Part V deals with constitutional jurisdiction over privacy in Canada. The Part assesses the merits of competing federal and provincial claims for jurisdiction over privacy matters and concludes that jurisdiction is probably shared by the two levels of government. The Part then discusses some of the conceptual and historical models for federal-provincial co-operation that might inform a shared approach to the regulation of privacy.

Constitutional Jurisdiction Over Privacy

Implicit throughout our discussion of the financial services sector in Canada is the role of the Canadian constitution and the division of powers over it. Into this difficult mix we must add an analysis of power over privacy *per se*. In essence, the federal government has power over banks because they are purely federal institutions. Banks will be subject to less provincial legislation than other institutions. The federal government has the power to incorporate and regulate insurers, trust companies, loan companies and cooperative credit associations. These institutions are subject also to extensive provincial regulation of their business and affairs. Some financial services providers are not regulated as financial institutions at all, and so are subject only to the general business laws of each province. Thus, some financial services providers are subject to the regulation of privacy which is imposed under the federal financial institutions laws, some subject to provincial regulation, if any, and some to no regulation of privacy whatsoever except, of course, to the extent they have operations in Quebec.

The federal government is discussing the introduction of laws to regulate privacy generally which, presumably, would apply to the financial services sector. The issue arises to what extent the federal government has the power to enact any such legislation, or whether it may do so in cooperation with the provinces.

It has been suggested by responsible commentators that the federal government has no power to enact privacy laws, even respecting matters under its jurisdiction, such as banks and federally incorporated trust companies and insurance companies. Based on our review of the law, this appears to overstate the case, but perhaps not by very much.

Sections 91 and 92 of the *Constitution Act*

The extent of federal and provincial jurisdiction over privacy generally, and over privacy as it relates specifically to financial institutions, is not an easy matter to determine: the heads of power in sections 91 and 92 of the *Constitution Act* do not contain anything that clearly and definitively

encompasses privacy either in a general sense or in the specific context of financial services.⁴⁵⁸ There is nothing in the “pith and substance” of privacy that associates it with any single federal or provincial power, given that it is an area that crosses many boundaries and has applications in different fields of endeavor – something that is at odds with the more discrete categories in the *Constitution Act*.⁴⁵⁹

To the extent that private information is disclosed to banks, it might be said to fall within federal jurisdiction over “Banking, Incorporation of Banks, and the Issue of Paper Money”, (s. 91(15)); “Savings Banks” (s. 91(16)); federally incorporated corporations under the federal government’s implied jurisdiction over works and undertakings extending beyond the province (s. 92(10)); “[t]he Regulation of Trade and Commerce” (s. 91(2)); or, possibly, criminal law (s.91(27)). The federal government also has jurisdiction over privacy as it relates to the federal public sector. Federal laws governing privacy matters could reasonably be classified as being ancillary to any of the foregoing heads of power, or, to use the formulation of Laskin J. A. (as he then was), displaying a “rational, functional connection” to one or more of these federal powers enumerated in s. 91 (and s. 92).⁴⁶⁰

This is not to say, however, that provincial heads of power listed in s. 92 are inapplicable as a result. The most obvious provincial power is “Property and Civil Rights in the Province” (s. 92(13)), which would logically extend to private information as a type of intangible personal property or to privacy as an enforceable private right as contemplated in s. 92(13). This head of power has been used to uphold the constitutional validity of consumer protection legislation, of which privacy legislation is clearly a variety.⁴⁶¹ There is also provincial jurisdiction over “[g]enerally all Matters of a merely local or private Nature in the Province” (s. 92(16)), although this categorization might be difficult to maintain given the fact that privacy concerns might easily cease to be merely local, or confined to a strictly provincial sphere, in any given instance. Provincial privacy laws might also be said to be ancillary or rationally connected to “[t]he Incorporation of Companies with Provincial Objects” (s. 92(11)), for example provincially incorporated insurance companies, trust or loan companies or co-operative credit associations. Here again, however, it is difficult to conclude that privacy falls exclusively within provincial jurisdiction, when there are contenders at least as strong in s. 91 as in s. 92.

Jurisdiction can be of a “double aspect”, *i.e.* competent to both the federal Parliament and to the provincial legislatures.⁴⁶² An example of a field with such a double aspect is highway traffic offences, where the provinces enforce their own legislation and where the federal *Criminal Code* also has jurisdiction. Other areas of dual jurisdiction are insolvency, securities regulation (generally a matter of provincial concern but also the subject of federal criminal sanction), maintenance of spouses and custody over children. In each of these examples, concurrent jurisdiction is exercised without undue conflict. There may be circumstances, however, where compliance with two levels of regulation may become impossible, in which case the doctrine of

⁴⁵⁸ *Constitution Act, 1982*.

⁴⁵⁹ *Union Colliery Co. v. Bryden* [1899] A.C. 580 (P.C.) at 587, *per* Lord Watson.

⁴⁶⁰ *Papp v. Papp* [1970] 1 O.R. 331 (Ont. C.A.) at 336.

⁴⁶¹ *Irwin Toy v. Quebec* [1989] 1 S.C.R. 927 at 953.

⁴⁶² *Hodge v. The Queen* (1883) 9 App. Cas. 117 (P.C.) at 130, *per* Sir Barnes Peacock.

paramountcy might justify exclusive federal jurisdiction.⁴⁶³ In our view, this is unlikely to be the case with the regulation of privacy.⁴⁶⁴

Federal Trade and Commerce Power

It appears to be very doubtful that the federal government could regulate privacy as it relates to financial services as a matter of exclusive federal jurisdiction. Any attempt to do so would presumably be by invoking one or more of the powers over economic life that are granted to it in s. 91. The first of these is the federal power over “[t]he Regulation of Trade and Commerce” (s. 91(2)), but it should be noted that this power has been narrowed to exclude such jurisdiction where it would conflict with “the power to regulate by legislation the contracts of a particular business or trade, such as the business of fire insurance in a particular province”.⁴⁶⁵ While there is this tension between federal power over trade and commerce and provincial jurisdiction over property and civil rights, it has been generally accepted that the trade and commerce power will apply to inter-provincial and international trade and commerce, as well as to what Sir Montague Smith called in *Citizens’ Insurance Co. v. Parsons* the “general regulation of trade affecting the whole Dominion.”⁴⁶⁶ Given that privacy concerns in the financial services sector are unlikely to be confined to wholly provincial entities or transactions, there is an argument that the federal government could use the trade and commerce power to justify exclusive jurisdiction over privacy respecting inter-provincial trade, there is a strong case for concurrent provincial jurisdiction based on the property and civil rights classification. It is also worth pointing out that the courts have not yet been willing to extend the trade and commerce power as widely as they might. Its application, as it relates to interprovincial trade (the first branch in *Parsons*), was rejected in two recent decisions of the Supreme Court;⁴⁶⁷ and as a general power of economic regulation (the second branch of *Parsons*) it has almost consistently been rejected.⁴⁶⁸ In *MacDonald v. Vapor Canada*, Laskin C.J.C. laid down three criteria for the application of the general trade and commerce power: (1) the presence of a “general regulatory scheme”; (2) the “oversight of a regulatory agency”; and (3) a concern “with trade as a whole rather than with a particular industry.”⁴⁶⁹ To these three criteria, Dickson C.J.C. added two more in *General Motors v. City National Leasing*: (4) “the legislation should be of a nature that the provinces jointly or severally would be constitutionally incapable of enacting”; and (5) “the failure to include one or more provinces or localities in a legislative scheme would jeopardize the successful operation of the scheme in other parts of the country”.⁴⁷⁰ With respect to privacy regulation in the financial services industry, only the first criterion would be satisfied. More importantly, it is difficult to

⁴⁶³ See Peter Hogg, *Constitutional Law of Canada* (Toronto, 1997) at 15-11 to 15-12 and 16-1 to 16-6.

⁴⁶⁴ For further discussion, see heading (d) Conclusion, below in this Part V.

⁴⁶⁵ *Citizens’ Insurance Co. v. Parsons* (1881) 7 App. Cas. 96 (P.C.) at 113, per Sir Montague Smith.

⁴⁶⁶ *Ibid.*; see also *Re Farm Products Marketing Act* [1957] S.C.R. 198 at 211-12.

⁴⁶⁷ *Dominion Stores v. The Queen* [1980] 1 S.C.R. 844; and *Labatt Breweries v. A-G. Canada* [1980] 1 S.C.R. 844 at 866. But see the discussion of these cases in Hogg, *supra*, note 463 at 20-9 to 20-10.

⁴⁶⁸ See *A.-G. Ontario v. A.-G. Canada* [1937] A.C.405 (P.C.); *Dominion Stores v. The Queen*; *Labatt Breweries v. A.-G. Canada*; *MacDonald v. Vapor Canada* [1977] 2 S.C.R. 134; *General Motors v. City National Leasing* [1989] 1 S.C.R. 641.

⁴⁶⁹ *MacDonald v. Vapor Canada*, *supra*, note 468 at 661.

⁴⁷⁰ *General Motors v. City National Leasing*, *supra*, note 468 at 679.

argue that the provinces would be constitutionally unable to enact legislation in this field, given their power over property and civil rights. And in view of the possibility of federal and provincial co-operation, it is difficult to suggest that a legislative scheme governing the collection, retention and disclosure of private information would be put at significant risk without exclusive federal competence in this area.

Peace, Order and Good Government

A further option for the federal government would be to argue that exclusive power to regulate privacy matters, either generally or as more particularly related to financial institutions, falls under the federal Parliament's power "to make Laws for the Peace, Order and good Government of Canada, in relation to all Matters not coming within the Classes of Subjects by this Act assigned exclusively to the Legislatures of the Provinces..." (s. 91). As has been suggested previously, privacy may not fall *exclusively* in provincial jurisdiction, which would in theory permit exercise of federal residual power over peace, order and good government ("POGG").

The first branch of the POGG power is the emergency branch, which is not relevant here, as it is unlikely that regulation of flows of confidential information is a concern so pressing that it would be considered an emergency demanding remedy through the exercise of the POGG power.⁴⁷¹

The second branch of POGG is the "gap" branch, which may be used to justify federal jurisdiction where this fills in lacunae in the distribution of powers between the federal parliament and the provincial legislatures.⁴⁷² This branch of POGG has been used to determine jurisdiction over matters not specifically enumerated in s. 91 or s. 92, such as aeronautics, atomic energy or the national capital region, or to make sense of inconsistencies in the text of the *Constitution Act* itself (e.g., the reference to companies with "Provincial Objects" in s. 92(10) but

no corresponding reference to companies with federal objects in s. 91).⁴⁷³ Peter Hogg notes, however, that the "gap" branch covers "limited and unusual cases" but is inappropriate where the subject matter of legislation is merely novel:

In most cases a "new" or hitherto unrecognized kind of law does not have any necessary or logical claim to come within p.o.g.g. It might come within property and civil rights in the province (s. 92(13)) or matters of a merely local or private nature in the province (s. 92(16)). Which head of power is appropriate depends on the nature of the "new" matter, and the scope which is attributed to the various competing heads of power[,] of which p.o.g.g. is only one.⁴⁷⁴

⁴⁷¹ See the discussion of emergency in Hogg, *supra*, note 463 at 17-18 to 17-27.

⁴⁷² *Citizens' Insurance v. Parsons; Re Regulation and Control of Radio Communication in Canada* [1932] A.C. 304 (P.C.) at 312.

⁴⁷³ *Johannesson v. West St. Paul* [1952] 1 S.C.R. at 292; *Ontario Hydro v. Ontario* [1993] 3 S.C.R. 327; *Munro v. National Capital Commission* [1966] S.C.R. at 663.

⁴⁷⁴ Hogg, *supra*, note 463 at 17-7.

The third branch of POGG relates to matters of a “national dimension” or of “national concern”.⁴⁷⁵ Viscount Simon stated in the *Canada Temperance Foundation* case that the “true test” for this branch of POGG will be found

in the real subject matter of the legislation: if it is such that it goes beyond local or provincial concern or interests and must from its inherent nature be the concern of the Dominion as a whole ... then it will fall within the competence of the Dominion Parliament as a matter affecting the peace, order and good government of Canada, although it may in another aspect touch on matters specially reserved to the provincial legislatures.⁴⁷⁶

The “national concern” branch requires first of all that a matter is of “import or significance to all parts of Canada”.⁴⁷⁷ Hogg suggests, however, that mere desire for uniformity of legislation will be insufficient to qualify as a national concern, unless uniformity is required as a result of provincial inability to deal effectively with a problem or where differing régimes in different provinces will prove counter-productive.⁴⁷⁸ Privacy legislation differs in many respects from province to province (Quebec, for example, is unique in regulating privacy beyond the public sector), but it is certainly arguable that difference of approach does not necessarily frustrate effective protection of privacy interests on a national level. Any discrepancies probably do not amount to a matter of national concern, or could be minimized through interjurisdictional co-operation.

In the *Anti-Inflation Reference*, Beetz J. held that POGG is applicable on the basis of national concern only where a “matter” of sufficient distinctness is at stake, not some vaguely defined subject of concern.⁴⁷⁹ This point was elaborated by Le Dain J. in *Crown Zellerbach*:

For a matter to qualify as a matter of national concern ... it must have a singleness, distinctiveness and indivisibility that clearly distinguishes it from matters of provincial concern and a scale of impact on provincial jurisdiction that is reconcilable with the fundamental distribution of legislative power under the Constitution.⁴⁸⁰

National concern may not, then, be used simply to extend federal jurisdiction where the federal government sees this as a convenient way of addressing a problem of large implications, in spite of provincial competence to deal with the issue.⁴⁸¹ All provincial power would be at risk if POGG were to be used in this way.

⁴⁷⁵ *Russell v. The Queen* (1882) 7 App. Cas. 829 (P.C.); *A.-G. Ontario v. A.-G. Canada* [1896] A.C. 348 (P.C.); *A.-G. Ontario v. Canada Temperance Foundation* [1946] A.C. 193 (P.C.); *Johannesson v. West St. Paul*; *Munro v. National Capital Commission*; *R. v. Crown Zellerbach* [1988] 1 S.C.R. 401.

⁴⁷⁶ *A.-G. Ontario v. Canada Temperance Foundation*, *supra*, note 475 at 205-06.

⁴⁷⁷ Hogg, *supra*, note 463 at 17-12 to 17-13.

⁴⁷⁸ *Ibid.*

⁴⁷⁹ *Re Anti-Inflation Act* [1976] 2 S.C.R. 373 at 457-8.

⁴⁸⁰ *Crown Zellerbach*, *supra*, note 475 at 432.

⁴⁸¹ W.R. Lederman, “Unity and Diversity in Canadian Federalism” (1975) 53 *Canadian Bar Review* 597.

A final requirement for satisfying the national concern branch of POGG is that of newness: as Pigeon J. held in *The Queen v. Hauser*,

...the most important consideration for classifying the Narcotic Control Act as legislation enacted under the general residual federal power [*i.e.*, POGG], is that this is essentially legislation adopted to deal with a genuinely new problem which did not exist at the time of Confederation and clearly cannot be put in the class of "Matters of a merely local or private Nature"⁴⁸²

— or, presumably, in the class of property and civil rights in the province. Hogg glosses this statement as a requirement for conceptual rather than historical newness.⁴⁸³ He concludes, incidentally, that the "newness" doctrine is "irrelevant and unhelpful" for the purposes of identifying areas of the federal residual power, but Pigeon J's judgment remains authoritative. While provincial legislation in the area of privacy and public concerns over improper use of confidential information are of relatively recent date (legislative protection of privacy interests would have seemed outlandish in 1867), it is questionable whether privacy legislation constitutes a conceptually new matter (compare atomic energy). Perhaps it would be more accurate to say that recent initiatives have extended the application of standards governing confidential information to new areas, but do not respond to a need that is itself novel. It is difficult, furthermore, to argue that privacy legislation, either generally or as it relates to financial institutions, "clearly cannot be put in the class of 'Matters of a merely local and private nature'" in Mr Justice Pigeon's phrase, or in that of "Property and Civil Rights in the Province".

Conclusion

In view of the fact that the *Constitution Act*, 1982 does not deal conclusively with jurisdiction over privacy in general (let alone privacy in the context of financial institutions), there may be shared jurisdiction over privacy as between the federal and provincial levels of government. The better argument may be that it is solely a matter of provincial jurisdiction except with respect to the federal public sector. As has been discussed, either level of government might claim jurisdiction under any one of a number of heads of power enumerated in ss 91 and 92. From the federal point of view these are those specifically related to banks and banking, federally incorporated companies and other works and undertakings beyond the provinces, banks, criminal law and trade and commerce; from the provincial perspective, companies with provincial objects, property and civil rights in the province and matters of a purely local and private nature in the province.

The federal government might seek to regulate privacy as an exclusive domain, either through the exercise of its general economic power over trade and commerce or through the national concern branch of the federal residual power (POGG). In either case, however, judicial limits placed on the extension of federal power by either of these means would probably prevent the federal government from successfully staking a claim for exclusive jurisdiction. As a practical and political matter, the Government of Canada might be loath to be seen to be usurping jurisdiction

⁴⁸² [1979] 1 S.C.R. 984 at 1000-01.

⁴⁸³ Hogg, *supra*, note 463 at 17-17.

where the provinces have already enacted legislation that is not demonstrably inadequate or likely to frustrate any legitimate federal privacy concerns. If general privacy is to be effected, it should be an area of federal-provincial co-operation, given that both levels of government have legitimate concerns over privacy issues and based on an understanding that flows of confidential information are borderless and therefore require a co-operative approach.⁴⁸⁴

So with respect to the financial services sector, the government can regulate federally regulated companies. The case for doing so is strong with respect to banking, in that even though privacy appears to be a provincial jurisdiction, it is also an element inherent in regulating banking and the intrusion into provincial jurisdiction would appear to be justified since it is only incidental in nature. A further example of this is the *Telecommunications Act*, which regulates privacy in respect of telecommunications companies. It might be conceivable that “information highway” type regulation, which clearly involves the use of telecommunications facilities and multi-jurisdictional trade, could justify a broader spectrum of regulation, but it is unlikely to extend to the practices of each information gatherer. But the result appears to be that the federal government is confident only to legislate within its patchwork of competence.

Models for Federal-Provincial Cooperation

In a unitary state, such as New Zealand or the United Kingdom, to effect regulation of privacy is straightforward. This is not the case in a federal system in which privacy relates to a wide variety of commercial sectors as well as different constitutional jurisdictions. The study of comparative federalism has yielded a number of models for co-operation between the national and sub-national levels of government, which are discussed briefly below.

The first model is one that takes the unitary state as its starting point, asserting the right of the national level of government to jurisdiction in the face of a competing claim by what in Canada would be the provincial level. In Canada, this is unlikely to be applicable and could only be achieved through some of the constitutional principles discussed in the previous chapter: the federal government’s general economic power over the regulation of trade and commerce, its residual power over “Peace, Order and good Government” or by means of the doctrine of federal paramountcy.⁴⁸⁵ Areas in which the federal government has asserted exclusive jurisdiction include atomic energy and aeronautics. The government of Canada may also seek to impose national standards in areas that are otherwise left to the provinces to regulate, for example in

⁴⁸⁴ For some models for federal-provincial co-operation, see “Some Lessons in Federal-Provincial Legislative Cooperation” and “Uniform Law Conference Privacy Act Deliberations” in Ian Lawson, *Privacy and the Information Highway: Regulatory Options for Canada* (Industry Canada: 1996), available at <http://strategis.ic.gc.ca/SSG/ca00265e.html>. See also William A.W. Neilson, “Interjurisdictional Harmonization of Consumer Protection Laws and Administration in Canada” in Ronald C.C. Cumming, ed., *Perspectives on the Harmonization of Law in Canada: Collected Research Studies of the Royal Commission on the Economic Union and Development Prospects for Canada* (Toronto, 1985), 76-87.

⁴⁸⁵ See the discussion in this Part V under the heading Constitutional Jurisdiction over Privacy, under the sub-heading Peace, Order and Good Government.

health care. Ronald C.C. Cuming has called this “induced harmonization”.⁴⁸⁶ Such a model for federal-provincial relations was perhaps most typical of the 1970s and 1980s, which Patrick Monahan has described as the period of “executive” or “unilateral” federalism, as opposed to the more co-operative approach of the 1960s.⁴⁸⁷ Gérald A. Beaudoin also notes an oscillation between centralist and decentralist forms of federalism in recent Canadian history.⁴⁸⁸ While the exercise of federal jurisdiction may be desirable from the point of view of uniformity of regulation, ease of administration and centralization of decision-making, there are a number of reasons why an approach borrowed from the unitary state may not be desirable or particularly effective. In the first place, there are judicial restraints on the assertion of exclusive federal jurisdiction, which have been discussed earlier in this Part. These will make a claim for exclusive jurisdiction difficult to bring into effect to the extent that federal claims fail to be compelling. Secondly, and perhaps more importantly, such an approach may not be ideal from the point of view of amicable federal-provincial relations, although it should be pointed out that an ostensibly more consultative and co-operative approach can descend into squabbling that fails to yield a common solution. Moreover, the ability to induce harmonization depends upon the power to persuade rather than the power to legislate. The power to persuade is tied to the federal purse strings, as is the case with standards for health care. It is worth noting that the federal government’s power to induce standards for health care is rapidly eroding as the size of transfer payments to support health care declines. We do not see any reason or justification to attach any transfer payment to privacy legislation.

In contrast to the executive or unilateral approach to federalism, the principle of “subsidiarity” adopted by the European Communities may pertain: the principle that jurisdiction should be assigned on the basis of efficiency to the national (or local) rather than the supra-national level.⁴⁸⁹ In contrast to the executive or centralist model of federalism, federal systems may choose a greater degree of sub-state autonomy, even to the point where the federation becomes a looser confederation, composed of essentially sovereign entities with (typically) economic links.⁴⁹⁰ Short of a confederal arrangement are other forms of decentralized federalism, for example the asymmetrical model, which gives some sub-state units greater powers than others at the same level (for example, Bavaria, which has powers not shared by other *Länder* within the

⁴⁸⁶ Ronald C.C. Cuming, “Harmonization of Law in Canada: An Overview” in Ronald C.C. Cumming, ed., *Perspectives on the Harmonization of Law in Canada: Collected Research Studies of the Royal Commission on the Economic Union and Development Prospects for Canada* (Toronto, 1985) at 25-28. See also William A.W. Neilson, “Interjurisdictional Harmonization of Consumer Protection Laws and Administration in Canada” in Ronald C.C. Cumming, ed., *Perspectives on the Harmonization of Law in Canada: Collected Research Studies of the Royal Commission on the Economic Union and Development Prospects for Canada* (Toronto, 1985) at 88.

⁴⁸⁷ Patrick Monahan, *The Charter, Federalism and the Supreme Court of Canada* (Toronto, 1987) at 144-149.

⁴⁸⁸ See Gérald A. Beaudoin, “Fédérations et confédérations,” in *Essais sur la Constitution* (Ottawa, 1979) at 67.

⁴⁸⁹ See Commission of the European Communities Directorate General for Economic and Financial Affairs, “One Market, One Money”, *European Economy* 44 (October 1990) at 33, cited in Thomas J. Courchene, *In Praise of Renewed Federalism* (C.D. Howe Institute, The Canada Round: A Series on the Economics of Constitutional renewal, no. 2) (Toronto & Calgary, 1991) at 7; Peter M. Leslie, *The Maastricht Model: A Canadian Perspective on the European Union* (Kingston, Ont., 1996) at 59-60.

⁴⁹⁰ Beaudoin, supra, note 488 at 65-74.

Federal Republic of Germany).⁴⁹¹ Asymmetrical federalism allows a further variant, competitive federalism, under which sub-state units are free to set their own standards and to compete in attracting industry, investment or immigration.⁴⁹² A degree of decentralization, to a greater or lesser extent, is compatible with the other six models for federal-provincial co-operation identified by Cuming, which are discussed briefly below. Privacy is an interesting problem in that its issues are very close to the personal rights of every citizen, and accordingly would be amenable to being dealt with at the local level in accordance with community standards. This is in direct conflict with any goal of economic efficiency, however, which would mitigate in favour of a national if not a supra-national set of standards. We do see competitive federalism operating by Quebec's enactment of a comprehensive privacy protection statute. In the competitive federalism model, jurisdictions compete for benefits, such as increased revenues to the state or political benefits such as jobs for voters. It is difficult to see what, if any, benefits Quebec will gain from its privacy law, and no province appears to be eager to vie for leadership in privacy protection. Arguably, protection of privacy could be a marginal factor in people's decision to locate, but it is unlikely to provide any significant role.

The second model identified by Cuming is that of mirror legislation, under which the national level of government enacts comprehensive legislation that is duplicated by the provincial or state levels and administered by a joint regulatory body.⁴⁹³ Canada attempted to adopt this model in the field of telecommunications, and may be groping towards it in securities regulation, but it has

⁴⁹¹ *Ibid.* See also: Preston King, *Federalism and Federation* (Baltimore, 1982), 24-38, 38-55; Richard Simeon and Mary Janigan, eds, *Toolkits and Building Blocks: Constructing a New Canada* (Toronto & Calgary, 1991), 120-2, 123-9, 133-9, 142-81; Bertus de Villiers, ed., *Evaluating Federal Systems* (Dordrecht, Boston & London, 1994); Daniel J. Elazar, ed., *Federal Systems of the World: A Handbook of Federal, Confederal and Autonomy Arrangements*, 2d edition (Harlow, Essex, 1994).

⁴⁹² The debate over competitive federalism (and whether this leads to a "race to the bottom", i.e. to the jurisdiction with the lowest standards) has been played out in the U.S. market for corporate charters, and to a much lesser extent in Canada: see W.L. Cary, "Federalism and Corporate Law: Reflections upon Delaware" (1974) 83 *Yale Law Journal* 663; R. Romano, "The State Competition Debate in Corporate Law" (1987) 8 *Cardozo Law Review* 709; C.M. Tiebout, "A Pure Theory of Local Expenditures" (1956) 64 *J. Pol. Econ.* 416; R.K. Winter, "State Law, Shareholder Protection, and the Theory of the Corporation" (1977) 6 *Journal of Legal Studies* 251; P. Dodd & R. Leftwich, "The Market for Corporate Charters: 'Unhealthy Competition' versus Federal Regulation" (1980) 53 *Journal of Business Law* 259; F.H. Easterbrook, "Antitrust and the Economics of Federalism" (1983) 26 *Journal of Law & Economics* 23; B. Baysinger & H. Butler, "The Role of Corporate Law in the Theory of the Firm" (1985) 28 *Journal of Law & Economics* 179; R. Romano, "Law as a Product: Some Pieces of the Incorporation Puzzle" (1985) 1 *J. Law Econ. & Org.* 225; J.R. Macey & G.P. Miller, "Toward an Interest-Group Theory of Delaware Corporate Law" (1987) 65 *Texas Law Review* 469; D.R. Fischel et al., "The Regulation of Banks and Bank Holding Companies" (1987) 73 *Virginia Law Review* 301; W.E. Oates & Robert M. Schwab, "Economic Competition among Jurisdictions: Efficiency Enhancing or Distortion Inducing?" (1988) 35 *J. Pub. Econ.* 333; Note, "To Form a More Perfect Union? – Federalism and Informal Interstate Competition" (1989) 102 *Harvard Law Review* 842; L.A. Bebechuk, "Federalism and the Corporation: The Desirable Limits on State Competition in Corporate Law" (1992) 105 *Harvard Law Review* 1435; R. Revesz, "Rehabilitating Interstate Competition: Rethinking the 'Race-to-the-Bottom' Rationale for Federal Environmental Regulation" (1992) 67 *New York University Law Review* 1210; R.J. Daniels, "Should Provinces Compete? – The Case for a Competitive Corporate Law Market" (1991) 36 *McGill Law Journal* 130 at 133-34; J.I. MacIntosh, "The Role of Interjurisdictional Competition in Shaping Canadian Corporate Law: A Second Look" *Law and Economics Working Paper Series 18* (Toronto: Faculty of Law, University of Toronto, 1993). See also Neil Guthrie, "'A Good Place to Shop': Choice of Forum and the Conflict of Laws" (1995) 27 *Ottawa Law Review* 201 at 204-5.

⁴⁹³ Neilson, *supra*, note 486 at 89-90. See also Lawson, *supra*, note 484.

not proved very successful in this country on the whole. In contrast, Australia has successfully implemented mirror legislation in the regulation of companies and securities at the state and federal levels.⁴⁹⁴

Jurisdictional abstention, the third model, involves a choice by one level of government not to intervene in a particular area, leaving the legislative and regulatory response to the other level. An example of such abstention is in the area of trade practices, where a number of provinces have refrained from enacting legislation, leaving the federal *Combines Investigations Act* to cover the field.⁴⁹⁵

Under the fourth or contract model, the national and sub-national governments negotiate the division of jurisdiction before they legislate, for example in agriculture.⁴⁹⁶ A related approach is conditional legislation, where sub-state levels have the option of adopting federal legislation in a given area or of adopting their own.⁴⁹⁷ Where there is no legislation at the state or provincial level, federal legislation automatically applies. This is the case, for example, with certain provisions of the *Combines Investigations Act*. One drawback of this model is that it can be seen to be coercive, as the short-lived *Borrowers and Depositors Protection Act* will demonstrate.⁴⁹⁸ The Government of Canada, concerned about the inconsistency of provincial legislation with respect to consumer protection, introduced the *Borrowers and Depositors Protection Act* in 1977 as a means of bringing about national standards. The federal government failed, however, to consult the provinces and financial institutions to a sufficient extent, and the bill was ultimately withdrawn as a result of severe criticism from those who felt that the bill intruded excessively on provincial jurisdiction, created duplication and confusion, and was not based on adequate consultation. A slightly different version of the conditional model would be that which allows the provinces to opt out of federal legislation, rather than in, and to legislate in areas that would otherwise be in the federal sphere. Examples are Quebec's own income tax and pension plan systems, which replace the federal scheme within the province. With this sort of arrangement, the contract model is clearly also applicable, as negotiation will have preceded the establishment of formal structures.⁴⁹⁹

A fifth model, which has perhaps been more typical of the Canadian experience, is that of concurrent legislation, where each level of government legislates with the knowledge that the other may do the same.⁵⁰⁰ Examples are corporate law, insolvency, family law and forestry. In many instances, two sets of legislation in a given field will not cause undue conflict (for example, in corporate law, where either the federal or provincial business corporations act will apply, depending on the vehicle chosen by the incorporator). In others, overlap may be more problematic, even to the point where the doctrine of paramountcy comes into play as a way of

⁴⁹⁴ See Neilson, *supra*, note 486 at 102-111.

⁴⁹⁵ *Ibid.*, at 90.

⁴⁹⁶ *Ibid.*, at 91.

⁴⁹⁷ *Ibid.*, at 91-92.

⁴⁹⁸ For the history of the short-lived bill, see Neilson, *supra*, note 486 at 76-82.

⁴⁹⁹ See the discussion in Courchene, *supra*, note 489 at 88. Courchene sees this as the basis for a renewed, decentralized federalism based on "concurrency with provincial paramountcy" at 86-92.

⁵⁰⁰ Neilson, *supra*, note 486 at 92-93.

resolving federal-provincial conflict. Often, benefits arise from competition among legal systems for clients.

A final model for federal-provincial co-operation is the collaborative or complementary model, which envisions interjurisdictional consultation as a way of co-ordinating legislation.⁵⁰¹ As Ian Lawson observes, this is often best achieved by working groups of senior bureaucrats, who meet in order to harmonize legislation and ensure that its implementation by the different levels of government is effective.⁵⁰² Ronald C.C. Cuming calls this "institutional harmonization", and observes that it may be brought about by the working groups of bodies like the Uniform Law Conference, the Canadian Bar Association and by the federal and provincial law reform commissions, as well as by bureaucratic committees.⁵⁰³ The collaborative model is clearly something that could be applied in conjunction with some of the other models, notably the contractual and conditional – even, he suggests, in areas where the federal government has exclusive jurisdiction.⁵⁰⁴ The collaborative model appears to be under investigation now, through the efforts of the uniform law conference to develop model legislation.

It is further possible for legislators to offer leadership in the marketplace. By causing federal institutions to enact and publicize privacy protection, they may raise marketplace standards so that institutions not subject to federal jurisdiction are forced to raise their own standards because of consumer demand. Of course, in the event consumer demand does not materialize, it is arguable that such protection is in any event unnecessary and that federally regulated institutions may have been put at a disadvantage. This may not, of course, realize all the federal government's public policy goals. A further means of implementation would be through standards of business practice promulgated by the Canada Deposit Insurance Corporation, a body of which many, but not all, deposit-taking provincial institutions are members. These standards are mandatory for members and compliance with them is monitored by regulatory agencies. It is, however, far fetched to suggest that privacy is incidental to deposit insurance, and member corporations already chafe under the burden of the CDIC standards.

⁵⁰¹ *Ibid.*, at 93-94.

⁵⁰² Lawson, *supra*, note 484.

⁵⁰³ Cuming, *supra*, note 486 at 31-47. See also his discussion of "bureaucratic harmonization" at 28-31.

⁵⁰⁴ Neilson, *supra*, note 486 at 93-94.

VI. Detailed Answers to Questions Posed

Introduction

Part VI provides detailed answers to the seven questions posed to the authors of this study. Part VI addresses the following issues: the adequacy of existing privacy legislation governing financial institutions; the need for additional protection as a result of new technologies and trends in financial services; the extent to which privacy regulation needs to be tailored specifically to the financial services sector; the degree to which the EU Directive and other foreign instruments create a need for additional privacy regulation, as a result of reciprocal provisions; the appropriate model for additional privacy regulation in Canada, if any; the lessons, if any, that can be learned from other efforts to introduce privacy protection in a multijurisdictional forum; and the risks to privacy that are posed by cross-ownership amongst financial institutions and the provision of multiple services by a single entity.

1. **Does existing privacy legislation governing Canadian financial services providers meet the privacy needs of consumers of financial services? If so, are such needs met consistently throughout the financial services industry, or in ways limited to certain types of financial services providers or those of certain jurisdictions?**

Sufficiency of existing protection

Existing privacy legislation governing federally regulated financial services providers is not extensive but it is augmented by common law and voluntary codes. The Draft Regulations are expected to increase the legal status of the voluntary codes. The consistency of such protection varies somewhat throughout the industry, appearing to be most highly developed amongst the big banks.⁵⁰⁵ It is probably true to say that there are more developed privacy policies amongst larger institutions. This is in part because they have larger administrations to handle privacy issues, and because they have a larger customer base of individuals than, say, a small provincial trust company providing services to corporate pension plans, or a Schedule II bank dealing principally with corporate customers. In general, both the low level of customer complaints about privacy and the nature of existing common law, equity and code-based provisions suggest that existing protection may be adequate.

Consistency Throughout the Sector

Existing privacy legislation and the common law and equity provide some protection for the privacy needs of consumers. However, privacy law outside Quebec is something of a patchwork quilt. Provisions in the federal statutes governing financial institutions require that directors adopt policies relating to confidentiality, that institutions take measures to prevent inaccuracies and unauthorized access, and that banks and insurance companies refrain from using customer

⁵⁰⁵ There are exceptions to these generalities and there is no evidence we are aware of that there are materially higher complaints for one type of institution, or one particular institution, than any other.

information in certain ways. We expect these federal provisions to be enhanced once the Draft Regulations come into force. Various pieces of provincial legislation include provisions that relate to information and personal privacy, including legislation which governs credit unions and legislation which governs consumer credit reporting. The common law protects privacy through the implied duty of confidentiality and through the possibility of invoking privacy codes as part of the contract between customer and institution. Outside the scope of the contract, various common law torts and equitable actions provide redress for privacy violations; however, legal and equitable actions are costly and time consuming, and it is often difficult to prove actual damages. In short, outside Quebec, the law protecting privacy is not as consistent as privacy experts might wish. But the costs of imposing additional privacy duties on institutions must be weighed against the benefits likely to be derived.

The adoption of privacy codes by financial institutions provides an additional degree of privacy protection.⁵⁰⁶ Privacy codes provide principles that govern the collection and were of personal information, and also establish individual rights of access to, and correction of, personal information. Although privacy codes are self-imposed, all indications are that institutions respect their terms and that such codes provide a reasonable framework for the protection of personal privacy.

It is important to note that federal regulation falls only on federal institutions. We have described elsewhere the extent to which provincial regulation of provincial institutions exists.⁵⁰⁷ However, there are large portions of the financial services sector which are largely unregulated in respect of informational privacy, except, of course, in Quebec. That is not to say that experience has shown that the practices of any of these companies requires further regulation. However, the customer financial information in the hands of a consumer finance company or a provincial loan company is no different in sensitivity than that in the hands of a bank.

Potential Areas of Improvement

As discussed elsewhere,⁵⁰⁸ certain measures could be taken to improve the existing model privacy codes against the ideal. Provisions might be added which provide further guidance on the use of implied consent, provide greater detail about the purposes for which information may be collected and when information may be collected from third parties, and clarify the reasons for the refusal of access to the individual's information. In addition, the codes should expressly permit an individual to opt out of programs which use personal information for direct marketing, and require institutions to take reasonable efforts to ensure that the individual's opt out request is effective.

Another concern is whether procedures to review complaints under privacy codes exist outside the institutions themselves. The banking industry has provided an external review mechanism in

⁵⁰⁶ For further discussion, see Part II under the heading Industry Association Codes.

⁵⁰⁷ See Part II under the headings Legislative Provisions Respecting Financial Institutions and Confidentiality, (b) Provincial Legislation.

⁵⁰⁸ See the measures discussed in this Part VII under the headings Privacy Codes, Standard Forms and Health Information.

the form of the Canadian Banking Ombudsman.⁵⁰⁹ The Ombudsman should provide some degree of independent review of privacy complaints, and so ensure that individual banks treat complainants fairly. However, the insurance, trust company and credit union industries do not have similar ombudsmen. An ombudsman *per se* may not always be an efficient solution; an insurance industry code provides access to mediation as a final step to resolve a dispute over privacy. This may be a practical and cost-efficient approach to the problem.

Finally, two further issues might be addressed by institutions, industry groups and, if necessary, regulators. First, existing standard forms used by institutions to obtain customer consent to access to and disclosure of personal information may be drafted too broadly. Such forms should generally be redrafted no more broadly than to allow the customer to consent only to access to and disclosure of personal information which is reasonably related to the relationship with the institution. Second, health information collected for insurance purposes should not be used for other purposes, such as the decision to approve or reject a credit application. The limited use of health information, collected in association with a loan application, for the evaluation of credit insurance related to that loan application ought to be expressly permitted.

2. To what extent will new technologies and/or internationalization of the delivery of financial services create a need for additional privacy protection?

To the extent that new banking technologies provide new channels for the delivery of financial services (such as PC- and Internet-based banking), the primary privacy implication appears to be concern for security of data communicated over computer or telecommunication networks.⁵¹⁰ For obvious reasons financial services providers typically go to great lengths to ensure data is securely transmitted, encrypted and stored. In any event, there are so many other needs relating to security of data, being transactional integrity and concerns for computer fraud, that in our view no legislation in favour of this aspect of the privacy interest is necessary.

It can be expected that in the future “data mining” will be used to a greater extent by Canadian financial institutions. Data mining has been cited as a new privacy concern. In fact, data mining in itself merely identifies aggregate results and patterns of behaviour that are useful to the financial institution’s marketing and product development. Arguably, compiling aggregate results is an activity which is not truly “personal” in nature, and so does not invoke a privacy interest *per se*. However, to the extent that such data mining techniques are further used to extract the names of persons to whom such lessons should be applied, and direct marketing is used to that end, privacy is affected. In order to ensure some degree of individual control over personal information, individuals should be permitted to opt out of targeted marketing activities. An institution should make reasonable efforts to ensure that the individual’s opt out request is effective.

⁵⁰⁹ For further discussion of the difficulties experienced in obtaining privacy codes from certain institutions, see Part II under the heading Industry Association Codes.

⁵¹⁰ For further discussion of new technologies and trends, see Part III.

Internationalization might militate in favour of additional regulation in two main respects. The first is if it becomes necessary to comply with higher privacy standards in order to ensure continuing transborder transfers of data into Canada from, for example, European Union states. The second is if financial institutions operating in Canada seek to use “data havens” for the off-shore storage or processing of data, in order to avoid the privacy measures that exist in this country. However, federally regulated financial institutions are currently restricted in their ability to transfer data out of Canada for processing purposes and must store certain types of information within Canada. As well, there has been no experience to date which suggests that financial institutions would seek to use data havens in this way, and it would seem unreasonable to expect that they would.

A further concern raised by internationalization is the possibility that individuals will provide data over the Internet to foreign financial services providers. However, it appears that, at this point, the options open to Canadian regulators are so limited that the rule is likely to be and remain *caveat emptor*.

3. To what extent does privacy regulation need to be tailored specifically to the financial services sector?

The question might be better put whether privacy regulation *should* be tailored specifically to the financial services sector. The issues concerning collection and handling of personal data are no different for financial institutions than for any other business. The processes are essentially the same. What is different is the sensitivity of individuals to data about their financial affairs and health.

To argue in favour of a tailored approach, one might note the financial services sector deals with health and financial records – two types of information that raise particular privacy concerns.⁵¹¹ The argument would run that privacy protection was necessary because of the adverse effects of inaccurate health and financial information and because of the sensitivity of such information. Perhaps only such sensitive forms of information require regulation, while other forms of information do not. On the other hand, because health and financial information is in fact sensitive, legal duties have grown up to protect it which to a large extent obviate the need for further regulation. It is in other spheres of human activity that the confidentiality of personal information has gained relatively little protection where regulation might be useful – assuming the kinds of information merit such protection in the first place.

Admittedly, the trend in Europe and elsewhere is to protect personal information on a comprehensive basis. That does not mean that the more measured, sectoral approach is wrong. However, there is unavoidable political pressure to justify departure from the comprehensive approach, particularly given the abstract nature of the privacy debate, which has been based on the benchmark of the OECD principles rather than the correction of particular privacy problems. As well, there is the possibility that “adequate” protection under Article 25 of the EU Directive

⁵¹¹ See the discussion of the Ekos Research Associates Inc. study at footnote 75 and accompanying text.

will require a uniform national standard of protection, although from initial indications this is far from certain.

4. Does the EU Directive, or potentially other legislation requiring reciprocal privacy protection, create a need for additional privacy regulation to facilitate transborder data flows?

Article 25 of the EU Directive states that transfers to third countries will be permitted only where there is an “adequate” level of protection in the third country, considered in light of all the circumstances surrounding the proposed transfer.⁵¹² The precise approach that European countries will take to the assessment of “adequate” protection is unclear and likely will remain that way, as the test inevitably involves some degree of judgment. The paper of the European Union Working Party identifies some of the factors that will be relevant to the decision but provides little guidance on how they will apply in particular cases. There are no present difficulties with data transfers and, in any event, indications are that financial services sector protection may well be “adequate”. In addition to Article 25, Article 26 of the EU Directive permits transfers to third countries without “adequate” protection where one of several exceptions applies, including where the data subject consents or where the transfer is necessary to perform a contract with the data subject or in the interests of the data subject.

Given the uncertainties involved in assessing “adequate” protection, it will be difficult for Canadian policymakers to predict what combination of domestic regulation, legislation and industry codes will meet the requirements of Article 25. The general approach to privacy protection set out in the EU Directive appears to owe much to European social and legal traditions, and may not sit well within Canada. Certainly, the EU Directive takes an approach that is significantly different from the sectoral approach to privacy regulation favored by the United States, our major trading partner. As a result, Canada may be best served by a policy approach to that does not seek to imitate the European model or level of privacy protection. Based on the German RailwayCard case,⁵¹³ it seems possible that many transfers of personal information between Europe and Canada could continue after the implementation of the EU Directive based on contractual privacy protection. If significant problems develop in the future, Canada’s privacy legislation and regulations may be adjusted to meet them.

⁵¹² For further discussion of the EU Directive, see Part IV.

⁵¹³ For further discussion of the German RailwayCard case, see footnotes 373 to 379 and accompanying text.

5. If the need is discovered for additional rules to protect privacy in the financial services sector, on which regulatory structure, given the Canadian context, should it be modeled?

Potential Regulatory Models

Assuming that it is determined that additional regulation to protect privacy is necessary, decision-makers must carefully consider which regulatory structure is best for the Canadian context. Several potential models exist.⁵¹⁴ For example, the United Kingdom provides the example of a system requiring registration before personal information may be processed. This has the advantage of permitting data subjects to consult a central registry listing all the institutions that use personal information. Quebec provides the example of a statute which does not require registration but sets out detailed privacy principles which must be followed by the private sector. In addition, complaints relating to private sector institutions may be taken to a government-established entity. New Zealand provides the example of a statute that sets out general privacy principles, which must be implemented by the private sector. The New Zealand law permits approved private sector codes to modify and replace the statutory duty to follow the privacy principles, although individuals may still bring privacy complaints to the New Zealand privacy commissioner. The model (or the mix of elements from different models) that should be chosen depends on a variety of factors, including the degree of cost, privacy protection and independent review which is desired by the policy maker.

On the degree of cost, a statute that sets out detailed privacy duties for financial institutions to follow will likely involve the highest degree of costs. It may also impose inappropriate obligations. The statute may use a particular approach or contain particular provisions that require the institution to change its internal procedures (such as its record-keeping methods) to ensure compliance. For example, the Quebec legislation requires institutions to establish a file on the individual for a stated purpose. However, institutions may have structured their information holdings so that there is no identifiable “file” for each person. Moreover, in an age of multiple uses of information and “data mining,” the records that do exist may have no single identifiable purpose. Rather, the information will be used according to the institution’s changing future needs and according to the particular associations and patterns that data mining programs might identify. As well, detailed statutory rights of access and correction – particularly if such rights contain short time limits and prohibit the charging of any fees for cost recovery – will impose additional administrative costs on financial institutions.

The question of the degree of privacy protection is intimately related to the question of the degree of cost. To better protect privacy, some privacy experts favour detailed statutory duties and restrictions. For example, such experts would favour duties requiring institutions to closely identify the future uses of information, answer requests for access to information within short time frames and at no cost to the requester, obtain written consent to particular uses wherever possible, and provide summaries of privacy policies to all customers. While these duties would ensure a relatively high level of privacy protection, they would impose new costs on institutions.

⁵¹⁴ For further discussion of the United Kingdom, Quebec and New Zealand models of legislation, see Part IV.

As well, other privacy measures might impose “cost” in the sense that financial institutions would be unable to use their information holdings in ways that would provide a competitive advantage. For example, some privacy experts would favour legislation that severely restricted the ability of a financial institution to data mine its information holdings and to restrict the institution’s ability to share information among subsidiaries or divisions providing different services. These costs are borne by consumers in the form of less developed services as well as administrative costs.

Most observers agree that an approach based on the OECD information principles or the Canadian Standards Association model privacy code is reasonable. The more difficult question is to what degree legislation should flesh out the principles and permit enforcement through institutional codes. For example, following the New Zealand approach, legislation might set out basic principles and leave the details of the application of these principles to approved industry codes. Or following the Quebec approach, the legislation itself might set out detailed provisions describing how privacy principles should be implemented in practice. Even if privacy provisions are spelt out in detail in legislation, there is a question what role industry or institutional codes might play in enforcement. For example, such codes might not replace the detailed provisions set out in legislation, but might be recognized as relevant interpretive aids in deciding how particular provisions apply to particular industries and situations. Relying on privacy codes to implement privacy principles, or to serve as aids in their interpretation, might ensure a greater degree of industry cooperation and self-enforcement. If privacy codes are to play a formal role in the implementation of legislation it could entail the establishment of some method of independent review to ensure that the codes fairly reflect privacy principles. For example, industry associations might be required to submit their codes to a review process before the federal Privacy Commissioner or the Office of the Superintendent of Financial Institutions. The review process might involve public hearings or submissions from consumer groups.

The question of the degree of enforcement and independent review relates both to cost and the degree of privacy protection. From the point of view of some privacy experts, the best method of enforcement would be an independent and government-established agency that was responsible for auditing the privacy practices of institutions and investigating and ruling on the privacy complaints of individuals. Of course, this approach will involve a higher degree of cost than an approach that relies to a great extent on self-enforcement. From industry’s point of view, a preferable approach would be a situation similar to the present situation, where institutions are largely responsible for their own compliance and complaints are resolved largely by internal procedures. An intermediate approach is one that would permit self-enforcement in most cases, but provide for review before an independent government agency to address complaints or problem areas. For example, individuals might be required to make complaints through the internal procedures of their institution; however, if the internal process did not satisfy the individual, they might have the right to approach the independent agency for an appeal or rehearing. In the Canadian context, this might mean that complaints that could not be resolved by institutions’ internal procedures could be taken to the federal Privacy Commissioner or to the Office of the Superintendent of Financial Institutions. Finally, another intermediate approach would be to require a system similar to the Canadian Banking Ombudsman for all sectors of the financial services industry. Industry associations would be required to establish arm’s length

Ombudsman offices; individuals unsatisfied by internal complaint processes could have their cases heard by the Ombudsman.

Choosing the Appropriate Model

This study has examined several models for privacy protection. All of them embody the OECD principles and, while advocates might argue about the strictness of one regime or the other, none of them have proven deficient in practice. It is, however, a reasonable inference that a large scale and rigid regulatory apparatus which imposes substantial expense is more likely to be wrong than a lighter, more flexible form of regulation. The application of a flexible approach is supported by our general observation about privacy regulation in the Canadian financial services sector: that there is a low level of privacy complaints and that existing model privacy codes generally conform to accepted privacy principles.

It would appear that the best regulatory model is one which provides for the greatest flexibility to adjust to changing circumstances. A system which permits rules to be developed and tailored at the industry level is likely to be the most appropriate. Some survey data indicates public distrust of self-regulation.⁵¹⁵ The distrust stems from the perception that there is a systemic privacy problem and from the fact that the regulator and regulated share the same identity. However, the self-regulation approach has given rise to the CSA model code, which is widely acclaimed and which embodies a high standard of privacy protection. The CSA principles have been incorporated into the Canadian Bankers Association's and other associations' model codes. In short, Canada's self-regulatory approach has not failed. Of course, there may be room for improvements to the existing system. Several possible improvements are discussed elsewhere in this study.⁵¹⁶

However, if it is decided to adopt a more stringent legislative approach to privacy protection – perhaps in order to comply with international pressure – an approach based on the New Zealand legislation would be appropriate.⁵¹⁷ Privacy principles would be set out in the legislation; these principles could then be enforced through approved industry codes rather than the legislation itself. Such an approach would provide for objective verification of industry codes, thus removing any taint of self-interest. Furthermore, it is our opinion that the present system of oversight would continue to be appropriate in such a system. The Canadian Banking Ombudsman should provide independent review of consumer complaints from the banking industry. Other industries could be encouraged to adopt measures that would provide for

⁵¹⁵ See footnotes 79 and 91 and accompanying text.

⁵¹⁶ These improvements include minor changes to existing privacy codes, the addition of provisions to privacy codes that permit individuals to opt out of “data mining” and targeted marketing programs, provisions to ensure that privacy codes are readily available to the public, new methods of review of unresolved privacy complaints, changes to standard forms to narrow their consent provisions and possible measures to ensure that health information collected for insurance purposes will not be used for other purposes. See Part II under the headings Industry Association Codes, (e) Observations on Association Codes; see also Part VII under the heading Privacy Codes.

⁵¹⁷ For further discussion of the New Zealand *Privacy Act*, see Part IV under the heading Privacy Legislation in New Zealand.

independent mediation or arbitration of privacy complaints which could not be resolved internally by institutions.

At several points in this study we have pointed to the efficacy of the market in dealing with privacy concerns. While it is not always readily accepted by advocates of regulation, the market is a potent force which may provide effective discipline of privacy-invading behaviour. The argument in favour of market forces has two main branches. The first branch is simply that customers have an interest in the privacy of their information and institutions have an interest in keeping customers. Accordingly, institutions and customers share an interest. (In addition, it should be noted that institutions themselves have an interest in the security and accuracy of their information holdings that exists apart from the interest of their customers.) The second branch of the argument is the proposition that consumers will complain if they perceive inadequate protection of privacy, and that institutions will respond to those complaints. In general, it appears that the present mix of market and common law restrictions on financial institutions works, based on the low level of complaints to institutions, ombudsmen and industry associations.

6. What lessons, if any, for Canada can be learned from other efforts to introduce broad privacy protection in a multijurisdictional forum?

There are not many examples of the enactment of privacy regimes in multi-jurisdictional for which are useful for Canadian purposes. The primary example is that of the European Union. However, the EU Directive must be approached somewhat warily from a Canadian perspective. In the first place, it was adopted primarily for the purpose of ensuring consistency of regulation for trade purposes – i.e., to ensure the easy transfer of data among European Union member states. No such risk confronts Canada at present.⁵¹⁸ Furthermore, the EU Directive arose as a compromise among several different national privacy laws and approaches. Canada does not have the same body of general privacy statutes as the European states. Moreover, the civil law legal system and European culture of these countries should lead us to treat the EU Directive as a document which is very much the product of its particular circumstances.⁵¹⁹

The experience with the EU Directive suggests that implementing a single directive that will apply to various states may involve a certain degree of compromise. Different states will want to ensure that certain features of their domestic privacy legislation are included (or at least recognized) in the directive. In the Canadian context, this suggests that the best results will be achieved if privacy policy is developed jointly with the provincial governments. Significant problems may arise in the case of Quebec, since that province has detailed privacy legislation which may not provide a workable model for the federal and other provincial jurisdictions.

⁵¹⁸ While the Quebec private sector privacy law contains provisions purporting to restrict the transfer of personal information out of the province, these provisions do not appear to have had a significant effect on data interprovincial transfers.

⁵¹⁹ To a certain extent, we should view Quebec's legislative experiment in the same light. Quebec's *Act to protect the privacy of personal information in the private sector* is a reflection of certain fundamental principles of conduct relating to privacy which were embodied in the recent revision of the province's *Civil Code*. However, the remaining common law jurisdictions in Canada do not share Quebec's unique culture and legal system.

Ideally, the same general level of protection should exist in all jurisdictions so that national institutions do not have to comply with multiple standards.

7. What risks do cross-ownership amongst financial institutions and the provision of multiple financial services by the same entity pose, if any, to privacy?

Cross-ownership amongst financial institutions creates the opportunity for sharing of information amongst marketers of different types of financial service to create more accurate marketing. As a single institution provides a larger number of products and services, it may use personal information for a greater number of purposes. As well, there could be a temptation to use certain types of information merely because they are available: for example, if medical or health records become widely available within an institution because of its insurance operations, such records may be used for new purposes. To the extent that this is a concern, it should be noted that, for instance, the Canadian Bankers Association code forbids the sharing of health information between a bank and its insurance subsidiary.⁵²⁰

Unfortunately, cross-ownership implications for different types of financial service is a very political issue. Therefore, it is important to separate competitive concerns from privacy concerns. There is a substantial lobby in Canada of independent insurance brokers, securities dealers and the like who see their competitive position threatened by the power of bank conglomerates. It is not the purpose of this study to address those competitive dynamics. The ability to share information amongst service providers or within different divisions of the same service provider has the potential to increase efficiencies and lower costs to consumers. Increased efficiencies typically result in pressures on less efficient participants in markets. It is not the purpose of this study to determine whether mitigation of the effects of such efficiencies is an advisable public policy goal. We are concerned, however, that restrictions on use of information to change the ability of a market participant to compete not be confused with restrictions on the flow of such information for privacy reasons. The degree and uncertainty of privacy concerns invites their exploitation by different lobbying factions. The privacy issues in different parts of the financial services sector do not differ materially. The issues of overlap of services and availability of information for different financial services are much more complicated than some participants would lead one to think. Government policy should not play a role in compounding those fears by commingling market regulation with privacy regulation.

In some cases, certain services are provided, for regulatory reasons, only through separate subsidiaries. In others, they may be provided through a single legal entity. Divisions between the various sectors, or pillars as they have been called, have largely dissolved. Selling insurance in bank branches is one of the few available networking arrangements which is legally restricted. The extent to which types of service are part of a single entity or not reflects an odd variety of historical accident and diverse policy, which does not include privacy, and the ingenuity of

⁵²⁰ Canadian Banking Association, *Privacy Model Code: Protecting individual bank customers' personal information* (1996), s. 5.4. In addition, the guidelines and model code adopted by insurance associations provide that insurance companies will not share information about insured persons with other institutions, except if certain narrow exceptions apply.

counsel and compliance officers in inventing new products around the restrictions. Insurance companies sell segregated funds, but these are mutual funds for all intents and purposes. They offer products that look a lot like deposits and have the power to issue credit cards. Securities dealers hold cash balances and pay interest on them, like deposits. In the United States, these are often transferable by cheque. Increasingly, different types of institutions are either going to look more and more alike, or be owned by the same entity and present one face to the public and be governed by one set of privacy and other internal policies. Think of CIBC Insurance, TD Trust, and Manulife Bank. Nevertheless, without consent, even in the case of common ownership, information cannot be shared amongst different legal entities. There does not seem to be any compelling logic for this, given that the separation of services into separate legal entities has nothing really to do with any interest of the customer in privacy, but rather with increased ability to regulate, prudential concerns or, most often, the efficacy of industry lobby groups in protecting their economic franchises. Thus, blanket consents on customer contracts which permit the sharing of information within a corporate group are justifiable.

Consumer groups have raised the concern that the use of information to try to sell other products could lead customers to feel obliged to buy those products if they are to maintain their banking services. In our view, this does not provide a basis for new regulation or policy. In the first place, it is not really a privacy concern. An institution is going to try to sell its products whether or not it uses personal information to do so. If an institution avails itself of customer information to make a targeted mailing to offer insurance to those most likely to buy the product, and thereby reduces costs by mailing out one-tenth of its usual number of letters, so much the better. If it has to mail out 10 times as many letters, the result is still that the same people with a pre-existing relationship with the institution are offered the opportunity to buy products. The argument really runs more to tied-selling concerns than privacy. There appears to be little if any evidence of anti-competitive tied-selling practices in the financial services sector.⁵²¹

⁵²¹ For further discussion of tied selling concerns, see Owens, Onyshko and Goode, *supra*, note 24.

VII. Conclusions

Introduction

Part VII sets out the authors' conclusions on the regulation of privacy as it relates to financial services providers. In particular, Part VII discusses privacy interests and the general need for regulation, existing privacy codes used in the financial services sector, standard forms used by financial services providers, the sharing of health information by insurers, the regulation of credit bureaux and insurance companies, the implications of the EU Directive, and the implications of new trends and technologies and the cross-ownership of financial services providers.

Privacy Interests and the Need for Regulation

Privacy interests arise in respect of the collection, use and communication of financial and health information in the financial services sector. These interests are addressed by existing legislation, common law and privacy codes. Further protection will be provided by proposed regulations under federal financial statutes pursuant to the provision therefore in the recently passed Bill C-82 (the "**Draft Regulations**"). Existing privacy protection relating to federally regulated financial services providers is not as strict as in some jurisdictions, such as the European Union countries, but is stricter than in some other jurisdictions, such as the United States. On the whole, the existing structure in Canada is one which embodies the principles and aspects of a modern privacy protection regime.

Given the low level of privacy complaints relating to financial institutions and the nature of existing privacy measures, a cost-benefit analysis would favour a conservative approach to future reforms. It should be noted, however, that to protect customer confidentiality and privacy institutions already engage in practices which would contribute to compliance with further regulation of privacy. Hence, it would be important to be clear about what additional costs would be incurred.

Because aspects of the privacy protection regime are stricter in some other jurisdictions such as the European Union countries, there may be pressure to establish a higher level of protection within Canada. If the decision were taken to do so, it would be essential to ensure that a flexible approach to implementing additional privacy measures is taken. The existing use of voluntary codes accommodates this principle. Other measures could be modelled on the approach of New Zealand's legislation,⁵²² for instance, which permits privacy codes of practice to be formulated in cooperation with data collectors most affected by them.

Regulation of privacy does not need to be tailored specifically to the financial services sector. The principles and concerns involved in protecting privacy are the same for financial services as for other sectors of the economy that collect, use and communicate personal information.

⁵²² For further discussion of the New Zealand *Privacy Act*, see Part IV under the heading Privacy Legislation in New Zealand.

However, the concerns may be different in terms of degree. As one would expect, surveys have shown that individuals are far more concerned about financial information and health information than other types of personal information.⁵²³ Accordingly, it could reasonably be decided to regulate only those areas of commercial endeavour that relate to financial and health information and consider further whether regulation is required for other, less sensitive types of information.

There is no difference in principle amongst the implications for privacy of the activities of any providers of financial services to individuals. The conclusions of this study are as applicable to consumer finance and credit card companies as they are for banks and insurance companies. There may be slight differences in degree, but the fundamental issues remain the same. However, the federal government appears to have no authority to enact rules with respect to privacy protection outside of the federally regulated financial services sector; as a result, privacy measures for consumer finance, credit card companies and the like, if any, would have to be imposed by provincial legislation. We are not aware of any course of conduct or body of complaints which presently needs to be addressed by such regulation in this sector. If provincial legislation or regulation is adopted, it is important to ensure consistency across Canada so that large entities which operate in different provinces are not subject to conflicting rules.

Privacy Codes

This study describes a number of informational privacy interests affected by the provision of financial services and which are recognized in privacy theory. Modern privacy principles – such as those set out in the OECD guidelines⁵²⁴ – address such interests. In Canada, these principles are embodied in privacy codes which have been adopted by industry associations and individual financial institutions. However, as discussed elsewhere in this study,⁵²⁵ some model codes might be improved by including provisions which provide further guidance on the use of implied consent, provide greater detail about the purposes for which information may be collected and when information may be collected from third parties, and clarification of the reasons for the refusal of access to the individual's information.

In addition, privacy codes should permit an individual to opt out of programs which use personal information for direct marketing, and require institutions to take reasonable efforts to ensure that the individual's opt out request is effective.⁵²⁶ The risk to privacy involved in direct marketing programs is not high. For instance, it is not equivalent to release of sensitive information. However, on a principled basis, it is appropriate to give individuals some ability to control the use of their information. In addition, unwanted attention by mail or telephone solicitation is a source of customer irritation and of increased concern about privacy. An "opt out" approach is

⁵²³ See the discussion of the Ekos Research Associates Inc. study at footnote 75 and accompanying text.

⁵²⁴ See footnote 15 and related text.

⁵²⁵ See Part II under the headings Industry Association Codes, (e) Observations on Association Codes.

⁵²⁶ It should be noted that some existing codes (including the Canadian Banking Association's model code) contain provisions which give the individual the ability to withdraw his or her consent to use information, subject to certain restrictions. In addition, the CBA code states that a bank will obtain the customer's consent before using personal information for marketing purposes. See footnotes 276 and 277 and accompanying text.

reasonable given the lack of any evidence of a serious privacy problem with respect to such practices. A greater level of privacy protection would be provided by an “opt in” approach, which would require an institution to obtain the customer’s explicit consent prior to any such use. However, an “opt in” approach will involve higher costs as consent must be collected from individual customers.

Some institutional privacy codes are not readily available to the public.⁵²⁷ Institutions and their customers would be best served if reasonable efforts were made to ensure that material about privacy codes was made available to the public on request. It could further be argued that institutions ought to deliver information to all customers about the protection of privacy afforded by the institution. If such a requirement were imposed, it should be in consultation with the industry, as we would guess that this would be a very costly effort and one which may be difficult to accommodate given the state of present information systems.

It is a typical provision of privacy protection regimes that individuals may take unresolved privacy complaints to a regulator or objective referee. In the case of the banking industry, the Canadian Banking Ombudsman plays this role.⁵²⁸ However, the banking industry has an enormous base of customers and transactions from which to support the role of the Ombudsman. It may not be efficient to establish similar industry ombudsmen for smaller groups of financial services providers. The answer may be for the model codes of industry associations to establish methods of mediation or arbitration to resolve specific disputes. For example, the IBC model code provides for an opportunity for independent mediation of refusals of customer access to information,⁵²⁹ a dispute resolution process of last resort which is relatively cost efficient since it does not necessarily entail a permanently sitting body. Industry associations (other than the Canadian Banking Association) could adopt a similar approach for complaints which are not resolved by the internal complaint procedure of the institution.

These observations on existing privacy codes do not represent significant shortcomings; rather, they represent areas for potential improvement against ideal notions of privacy protection. Generally, the Canadian model codes reflect the established privacy principles and the measures necessary to ensure their implementation.⁵³⁰ The codes represent the basis for a reasonable system of self-regulation which has been established by the main industry associations for the financial services sector.

⁵²⁷ For further discussion of the difficulties experienced in obtaining privacy codes from certain institutions, see Part II under the heading Industry Association Codes.

⁵²⁸ For further discussion of the role of the Canadian Banking Ombudsman, see footnotes 95 and 96 and accompanying text and footnotes 296 and 297 and accompanying text.

⁵²⁹ Insurance Bureau of Canada, *Model Personal Information Code* (1996), s. 4.9.1.

⁵³⁰ The extent to which model codes apply privacy principles is set out in the charts in Appendix A.

Standard Forms and Health Information

An area that should be addressed by institutions, industry associations and, if necessary, by regulators, is the wording of standard forms used by financial services providers. Industry forms and agreements that authorize the collection or sharing of personal information should respect, and not vitiate, the principles regarding the use and collection of such information established in the privacy codes.⁵³¹ Institutions need the customer's consent to the collection and sharing of information wherever reasonable and necessary but, in general, consent should be limited to certain types of circumstances or certain types of parties. For example, forms used by banks should permit access to or sharing of personal information for purposes related to the relationship between the bank and the customer. Provisions permitting access to or sharing of information for *any* purpose could be better replaced with more narrowly drafted provisions.

Health information collected for insurance purposes should not be used to make credit decisions.⁵³² Of course, certain health information is relevant to credit applications but should be collected and used specifically for that purpose and in that context. This concern is addressed by provisions in existing privacy codes. The Canadian Bankers Association model code states that banks will collect health information only for specific purposes – and that neither banks nor their subsidiaries or affiliates will share health information.⁵³³ As well, the guidelines and model code adopted by insurance associations provide that insurance companies will not share information about insured persons with other institutions, except if certain narrow exceptions apply.⁵³⁴ However, a provision in the Credit Union Central of Canada's draft privacy code permits the use of medical information collected by a credit union for both credit and related insurance purposes.⁵³⁵ Presumably, "related" in this context refers to credit insurance relating to the credit in respect of which health information has been given, a use which would seem to be appropriate. In general, the interest that both insurers and credit granters have in maintaining the integrity and candour of the information gathering process is so great that each would be unlikely to risk creating a perception that information was used for a purpose unrelated to its collection. We are not aware of any pattern of misuse of health information in the industry.

⁵³¹ For an analysis of certain banking forms, see footnotes 136 to 141 and accompanying text.

⁵³² For further discussion, see footnotes 283 to 285 and accompanying text.

⁵³³ Canadian Banking Association, *Privacy Model Code: Protecting individual bank customers' personal information* (1996), s. 5.4.

⁵³⁴ Canadian Life and Health Insurance Association, *Right to Privacy: Guideline No. 96*, s. 6; Insurance Bureau of Canada, *Model Personal Information Code* (1996), s. 4.3.2.

⁵³⁵ Credit Union Central of Canada, *Credit Union Code for the Protection of Personal Information* (Draft) (1996), s. 5.4.

Credit Bureaux and Insurance Companies

Two further issues should be addressed at the provincial level.⁵³⁶ Credit bureaux raise particular informational privacy concerns, given the importance of their function in the modern economy and the direct effect that credit reports may have on individuals. Credit bureaux are generally, but somewhat inconsistently, regulated at the provincial level. Statutory provisions requiring that individuals be informed of the use of a credit bureau, of the location and the contact person for the credit bureau, and of the right to see any credit bureau report are generally advisable. In addition, the sharing of health information by insurers through the Medical Information Bureau (MIB) may be a practice which should be regulated, in the same way that the sharing of information by credit bureaux is. Reform measures adopted by different provinces should be consistent.

Implications of the EU Directive

Indications are that there are no existing problems with transfers of personal data between the European Union and Canada. Moreover, there is little experience with the EU Directive⁵³⁷ as it is not fully implemented in Europe. It would be a mistake to look to the nascent and culturally specific privacy regime established by the EU Directive as necessarily providing leadership for Canada. The existing measures taken by the financial services sector, particularly if given further legislative sanction through the proposed Draft Regulations, may well qualify as “adequate” protection for the purposes of Article 25 of the EU Directive. The Canadian federally-regulated financial sector may qualify for “partial white-listing,” to use the words of the recent position paper of the EU Working Party.⁵³⁸ In any case, there is considerable uncertainty over how to comply with the Article 25 of the EU Directive. To improve the likelihood of compliance with Article 25 would be to move in the direction of more rather than less regulation, at a time when we do not know exactly what level of protection would qualify as “adequate.”

Trends, Technology and Cross-Ownership

In addition to the above, there are privacy issues relating to technologies and trends and to the cross-ownership of financial institutions.⁵³⁹ New technologies and trends generally do not raise privacy issues that require, at this point, a regulatory response. However, the increased use of “data mining” for direct marketing programs suggests that individuals should be permitted to opt out of such programs by providing notice to their institution. Cross-ownership of institutions may permit personal information to be used by different divisions of a single institution for a wider range of purposes. However, in our view, cross-ownership does not pose a significant risk to privacy interests to warrant special privacy regulation beyond that recommended elsewhere in this study.

⁵³⁶ For further discussion of these issues, see Part II under the headings Legislative Provisions Respecting Financial Institutions and Confidentiality, (b) Provincial Legislation.

⁵³⁷ For further discussion of the EU Directive, see Part IV.

⁵³⁸ For further discussion of the EU Working Party’s paper, see footnote 366 and accompanying text.

⁵³⁹ For further discussion of technologies and trends, see Part III.

Appendix A: Summary and Detailed Comparison Charts: A Comparison of Industry Privacy Codes and Certain Legislation

The attached is a chart which attempts to summarize the extent to which each of several privacy codes and pieces of legislation complies with certain principles respecting the protection of personal data. Depending upon the nature of the comparison, the result is cited either as a matter of degree (“Low”, “Medium”, “High”) or as to whether or not a particular provision is included at all (“Yes”, “No”). The chart is to a certain extent inherently misleading. It represents, first of all, an unavoidable exercise of subjective judgment. Second, the differences between one degree or another are often so slight as to be virtually insignificant. Third, it is misleading to suppose that there is a perfect embodiment of every principle, a departure from which represents a failure in will to protect privacy. The circumstances in which business is carried on involve several factors in adapting a principle to practice, including realistic cost benefit analysis, as well as any self interest in the economic value of data sharing. The assessments of degree of compliance are relative to the strictest practice embodying a particular principle, rather than an evaluation of the extent of the embodiment of the principle itself. It should also be noted that a rating of “Low” is not necessarily a negative rating. The strictest level of compliance may in certain circumstances be impractical. The UK *Data Protection Act*, for instance, provides for a civil action relating to inaccuracy of data. That is using the full force of the law for enforcement and therefore achieves a high rating, but it is an impractical remedy given the cost and slowness of the courts. In some instances, this is evidenced by all industry codes having a low level of compliance, a level in fact which is fully “compliant” but which omits some of the excessive provisions of the strictest embodiment of a standard.

Summary Comparison Chart (E.U., Quebec, C.B.A., CLHIA, I.B.C.)

Characteristic ⁵⁴⁰	European Union <i>Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995)</i>	Quebec <i>An Act respecting the protection of personal information in the Private Sector, R.S.Q. P. 39.1 (1994)</i>	Canadian Bankers Association <i>Privacy Model Code (1996)</i>	Canadian Life and Health Insurance Association <i>Right to Privacy Guideline No. 96</i>	Insurance Bureau of Canada <i>Model Personal Information Code (1997)</i>
1. Type of Document	European Union Directive	Legislation applying to the private sector in Quebec	Model code for banks	Model guidelines for life and health insurers	Model code for property and casualty insurers
2. Application	Public & private sector	Private sector	CBA members	CLHIA members	P&C insurers that adopt the Code
3. Enforcement	High	High	Medium	Low	Low-to-Medium
4. Personal information defined	Yes	Yes	Yes	Yes	Yes
5. Consent defined	Yes	Yes	Yes	No	Yes
6. OECD Collection Limitation Principle	Medium	High	Medium	Low	Medium
7. OECD Data Quality Principle	High	Medium-to-High	Medium	Medium-to-High	Medium
8. OECD Purpose Specification Principle	High	Medium-to-High	Low	Low	Low
9. OECD Use Limitation Principle	High	High	High	High	Medium
10. OECD Security Safeguards Principle	High	Medium	Medium	Medium	Medium
11. OECD Openness principle	High	Low	Medium	Low	Medium
12. OECD Individual Participation Principle	High	High	Medium	Low	Medium-to-High
13. OECD Accountability Principle	High	High	Medium	Low	Low-to-Medium

⁵⁴⁰ The assessments included in this Chart generally represent only fine graduations of a principle, and reference should be made to the attached, detailed chart and to the cover note to put such distinctions in proper perspective.

Characteristic ⁵⁴⁰	European Union <i>Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data</i> (1995)	Quebec <i>An Act respecting the protection of personal information in the Private Sector, R.S.Q. P. 38.1</i> (1994)	Canadian Bankers Association <i>Privacy Model Code</i> (1996)	Canadian Life and Health Insurance Association <i>Right to Privacy Guideline No. 96</i>	Insurance Bureau of Canada <i>Model Personal Information Code</i> (1997)
14. Specific Provisions on Consent	Low	High	Medium	Low	Medium
15. Provisions Restricting Transfer Outside the Jurisdiction	Yes	Yes	No	No	No
16. Special Features of Interest	Yes There are special measures that relate to the processing of personal data, the processing of sensitive data, and automated decision-making.	Yes There are special measures that relate to "nominative lists," which are defined as lists of "names, addresses or telephone numbers of natural persons." (s.22)	No	No	No

Summary Comparison Chart (TCAC, CUCC, CSA, U.K., N.Z.)

Characteristic ⁵⁴¹	Trust Companies Association of Canada Customer Privacy Code (1993)	Credit Union Central of Canada Credit Union Code for the Protection of Personal Information, Draft (1996)	Canadian Standards Association Model Code for the Protection of Personal Information (1996)	The United Kingdom Data Protection Act 1984 (c. 35)	New Zealand Privacy Act 1993
1. Type of Document	Model code for trust companies	Draft model code for credit unions	Model code for use by a business	Legislation, based on the OECD principles	Legislation, based on the OECD principles
2. Application	Trust companies that adopt the Code	Credit unions that adopt the Code	Businesses that adopt the Code	Public and private sector	Public and private sector
3. Enforcement	Low	Low-to-Medium	Low	High	High
4. Personal information defined	Yes	Yes	Yes	Yes	Yes
5. Consent defined	No	Yes	Yes	No	No
6. OECD Collection Limitation Principle	Medium	Low-to-Medium	Low-to-Medium	Medium-to-High	Medium-to-High
7. OECD Data Quality Principle	Medium-to-High	Medium	Medium	High	High
8. OECD Purpose Specification Principle	Low	Low	Low	High	Medium-to-High
9. OECD Use Limitation Principle	Medium	Medium	Medium	High	Medium
10. OECD Security Safeguards Principle	Medium	Medium	Medium	Medium	Medium
11. OECD Openness principle	Low	Medium	Medium	High	High
12. OECD Individual Participation Principle	Medium	Medium	Medium	High	High
13. OECD Accountability Principle	Low	Low-to-Medium	Low	High	High
14. Specific Provisions on Consent	Low	Medium	Medium	Low	Low
15. Provisions Restricting Transfer Outside the Jurisdiction	No	No	No	Yes	No
16. Special Features of Interest	No	No	No	Yes	Yes

⁵⁴¹ The assessments included in this Chart generally represent only fine graduations of embodiment of a principle, and reference should be made to the attached, detailed chart and to the cover note to put such distinctions in proper perspective.

Detailed Comparison Chart (E.U., Quebec, C.B.A., CLHIA, I.B.C.)

Characteristic	European Union <i>Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995)</i>	Quebec <i>An Act respecting the protection of personal information in the Private Sector, R.S.Q. P. 39.1 (1994)</i>	Canadian Bankers Association <i>Privacy Model Code (1996)</i>	Canadian Life and Health Insurance Association <i>Right to Privacy Guideline No. 96</i>	Insurance Bureau of Canada <i>Model Personal Information Code (1996)</i>
1. Type of Document	EU Directive which is to be adopted by European Union members into national legislation.	Legislation applying to the private sector in Quebec, based on the OECD principles. Note that the public sector is covered by earlier access and privacy legislation.	Model code for banks, based on the CSA Model Code principles. The CBA Code comes in the form of several principles with subpoints that provide further discussion.	Model guidelines for life and health insurers, based on the OECD principles. The Guidelines are accompanied by Notes that provide further discussion.	Model code for property and casualty insurers, based on the CSA Model Code principles. The IBC Code comes in the form of several principles with subpoints that provide further discussion.
2. Application	The EU Directive applies to both the private and public sector.	Private sector The Act applies to the private sector in Quebec generally.	CBA members The Code states that CBA members shall have privacy codes that comply with the Code.	CLHIA members The Guidelines state that they are intended as a minimum standard for CLHIA members.	P&C insurers that adopt the Code
3. Enforcement	High Enforcement of the EU Directive's provisions is by judicial remedy available to individuals and by public authorities.	High Enforcement of the Act is by the Quebec access and privacy commission.	Medium Enforcement of the Code is by privacy policies and complaint procedures established by banks. However, individuals unsatisfied by the bank's complaint process may complain to the Canadian Banking Ombudsman.	Low Enforcement of the Guidelines is by privacy policies and complaint procedures established by insurers.	Low-to-Medium Enforcement of the Code is by privacy policies and complaint procedures established by insurers. In the case of denials of information, the Code raises the possibility of mediation before an independent party.
4. Personal information defined	Yes "[P]ersonal data' shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." (Art. 2.)	Yes "Personal information is any information that relates to a natural person and allows that person to be identified." (s. 2)	Yes "Information about an individual customer of the bank. Includes but is not limited to the individual's name, address, age, gender, identification numbers, income, employment, assets, liabilities, source of funds, payment records, personal references and health records. May also identify whether or not credit was extended and to whom the bank disclosed the information." (Definitions)	Yes "[P]ersonal information' means any information relating to an identified or identifiable individual, including, but not limited to, health and financial information." (s. 2) The Notes state: "Personal information' applies to identified or identifiable information and does not include statistical and other unidentifiable data."	Yes "Information about a customer that is recorded in any form. It may include an individual's name, address, telephone number, date of birth, family status, marital status, occupation, medical and health records, assets, liabilities, income, credit rating, whether or not credit was extended or refused to the individual, credit and payment records of the individual, an individual's previous insurance experience including claims history, and an individual's driving record." (Definitions)

Characteristic	European Union <i>Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995)</i>	Quebec <i>An Act respecting the protection of personal information in the Private Sector, R.S.Q. P. 39.1 (1994)</i>	Canadian Bankers Association <i>Privacy Model Code (1996)</i>	Canadian Life and Health Insurance Association <i>Right to Privacy Guideline No. 96</i>	Insurance Bureau of Canada <i>Model Personal Information Code (1996)</i>
5. Consent defined	Yes "1) The data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." (Art. 2.)	Yes "Consent to the communication or use of personal information must be manifested, free, and enlightened, and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purposes for which it was requested. Consent given otherwise than in accordance with the (above) is without effect." (s. 14.)	Yes "Voluntary agreement. Consent can be expressed, implied, or provided through an authorized representative. A customer can express consent explicitly, orally, in writing or electronically. Express consent is unequivocal and does not require inference by the bank seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the customer." (Definitions)	No	Yes "Voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent can be given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the P&C insurer seeking consent. Implied consent arises where consent may reasonably be inferred from action or inaction of the customer." (Definitions)
6. OECD Collection Limitation Principle There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.	Medium Data must be collected for "specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." (Art. 6.)	High To collect personal information the business must establish a tie on the individual and do so for a serious and legitimate reason. (s. 4) A business may collect only information "necessary" for the object file. (s. 5) A business may not refuse to respond to a request for goods or services or a request relating to employment because the applicant refuses to disclose personal information, except where: collection of the information is necessary for the conclusion or performance of a contract; collection of the information is authorized by law, or there are reasonable grounds to believe the request is not lawful. (s. 9)	Medium "Banks will limit the amount and type of personal information they collect. They will collect personal information for the purposes they have already identified to the customers. Banks will collect personal information using procedures that are fair and lawful." (Pr. 4) Banks will collect information only: to understand the customer's needs; to determine the suitability of products or services for the customer or the customer's eligibility; to set up and manage products and services that meet the customer's needs; to provide ongoing service; to meet legal and regulatory requirements. (s.2.2)	Low "Only lawful means will be used to collect personal information. Every reasonable effort will be made to ensure that personal information obtained by the company is: (a) pertinent to the effective conduct of the company's business. ..." (s.4)	Medium "The collection of personal information shall be limited to that which is necessary for the purposes identified by the P&C insurer. Information shall be collected by fair and lawful means." (s.4.4) The insurer will collect personal information only for establishing and maintaining communications with customers; underwriting risks on a prudent basis; investigating and paying claims; detecting and preventing fraud; offering and providing products and services to meet customer needs; compiling statistics; complying with the law; and a business or activity which it may undertake under applicable federal, provincial or territorial legislation. (s.4.2.1.)

Characteristic	European Union <i>Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data</i> (1995)	Quebec An Act respecting the protection of personal information in the Private Sector, R.S.Q. P. 39.1 (1994)	Canadian Bankers Association <i>Privacy Model Code</i> (1996)	Canadian Life and Health Insurance Association <i>Right to Privacy</i> Guideline No. 96	Insurance Bureau of Canada <i>Model Personal Information Code</i> (1996)
7. OECD Data Quality Principle Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.	High Data must be processed "fairly and lawfully." Data must be "adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed." Data must be "accurate and, where necessary, kept up to date." (See Art. 6.)	Medium-to-High Information must be up-to-date and accurate when used to make decisions. (s. 11)	Medium "Banks will keep personal information accurate, complete, current and relevant as necessary for its identified purposes." (Pr. 6) Banks will take reasonable efforts to "minimize the possibility" of using inaccurate, incomplete or outdated information when making a decision about the individual.	Medium-to-High "Every reasonable effort will be made to ensure that personal information obtained by the company is: (a) pertinent to the effective conduct of the company's business; (b) as accurate and complete as possible consistent with the purpose(s) for which it was obtained;" (s. 4) The Notes state that the intent of the data quality section is "to ensure that data is collected only from reliable sources and that only pertinent information is collected."	Medium "Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is used." The extent to which information must meet the above standard will depend on the use of the information, taking into account the interests of the customer. Information should be sufficiently accurate, complete and up-to-date to "minimize the possibility" inappropriate information may be used to make a decision.
8. OECD Purpose Specification Principle The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.	High If data are collected from the data subject, then the data controller must provide: the identity of controller; the purposes of processing of the data; other information such as the recipients of data, whether replies by the individual are obligatory and the possible consequences of a refusal to reply, and the existence of the right of access and rectification of data. (Art. 10.) Where the data are not collected from the data subject, the data controller still has a duty to provide information to the data subject at the time of undertaking the recording of the data or disclosure of data to a third party. (Art. 11.)	Medium-to-High A business which collects information directly from the individual must inform the individual of the object of the file, the use of information and categories of people with access, the place where the file is kept and the individual's rights of access and rectification. (s. 8) A business having as its object the lending of money, which consults credit reports, must inform the subject individual of his or her right of access to and rectification of the report held by the credit bureau. The business must communicate the content of the credit report consulted for the purpose of making a decision about the individual. (s. 19)	Low "Banks will identify the purposes of collecting personal information, before or when it is provided." (Pr. 2) Banks will collect information primarily from customers, but also from sources such as credit bureaus, employers and other lenders. (s.4.2)	Low "The purpose(s) for which personal information is collected from an individual will be specified on or before the collection of the information, and any change of purpose will be communicated to the individual." (s. 5) The Notes state that if an authorization is received to obtain information for underwriting and claims purposes, such information may not be used for unrelated purposes without the individual's knowledge.	Low "The purposes for which personal information is collected shall be identified by the P&C insurer before or at the time the information is collected." (Pr.4.2) Insurers will obtain personal information primarily from insurance customers, but also from sources such as other P&C insurers, brokers and underwriting or claims networks. (s.4.4.1)

<p>Characteristic</p>	<p>European Union <i>Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data</i> (1995)</p>	<p>Quebec <i>An Act respecting the protection of personal information in the Private Sector, R.S.Q. P. 39.1</i> (1994)</p>	<p>Canadian Bankers Association <i>Privacy Model Code</i> (1996)</p>	<p>Canadian Life and Health Insurance Association <i>Right to Privacy</i> Guideline No. 96</p>	<p>Insurance Bureau of Canada <i>Model Personal Information Code</i> (1996)</p>
<p>9. OECD Use Limitation Principle Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the purpose specification principle] except: (a) with the consent of the data subject; or (b) by the authority of law.</p>	<p>High Personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." Further processing for historical, statistical or scientific purposes will be considered compatible purposes if safeguards are provided. (See Art. 6.)</p>	<p>High A business cannot communicate or use information for purposes not relevant to the object of the file, unless permitted by the Act or the individual consents. (s. 13) There is a set of more than a dozen exceptions that allow communication of information without the individual's consent. (s. 18) A special section permits communication of information for research purposes. (s. 21) Once the object of a file has been achieved, no information in the file may be used other than with the consent of the individual, subject to any time limit or retention schedule established by regulation. (s.12)</p>	<p>High "Banks will use or disclose personal information only for the reasons it was collected, unless a customer gives consent to use or disclose it for another reason. Under certain exceptional circumstances, banks have a common law duty or right to disclose personal information to protect the bank's or the public interest without customer consent. Banks will keep information only as long as necessary for the identified purposes." (Pr.5) The subpoints under Principle 5 permit disclosure or use in various circumstances. They also set out special provisions for health records. Health records will be collected only for specific purposes. Banks and subsidiaries will not disclose health records to each other. "For example, a bank will not be able to use a subsidiary's customer health records to help assess a loan application." (s.5.4)</p>	<p>High "Personal information will not be disclosed or used for purposes other than those specified to the individual in accordance with section 5, except: (i) with the consent of the individual concerned; or (ii) where reasonably necessary to determine eligibility for an insurance benefit, or to protect the interests of the company against criminal activity, fraud, and material misrepresentation in connection with an insurance contract; or (iv) in discharge of public duty." (s.6) The Notes state that an authorization included on the application plan may permit disclosures to specified entities (such as the employer) or for specified reasons. As well, information may be used or disclosed without consent where subpoenaed or where an investigation or surveillance is undertaken because of suspicion of fraud or for preparation for legal proceedings.</p>	<p>Medium "Personal information shall not be used or disclosed for purposes other than those for which the information was collected, except with the consent of the customer or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes." (s.4.5) However, there are identified situations in which P&C insurers will disclose personal information "as dictated by prudent insurance practices": for purposes of sharing risk with other insurance companies; for underwriting claims, classification and rating purposes; to businesses that provide goods and services to insurance companies and customers such as data processors, loss controllers and claims adjusters; and to insurance intermediaries such as brokers and agents. (s.4.5.1)</p>

Characteristic	European Union <i>Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995)</i>	Quebec <i>An Act respecting the protection of personal information in the Private Sector, R.S.Q. P. 39.1 (1994)</i>	Canadian Bankers Association <i>Privacy Model Code (1996)</i>	Canadian Life and Health Insurance Association <i>Right to Privacy Guideline No. 96</i>	Insurance Bureau of Canada <i>Model Personal Information Code (1996)</i>
10. OECD Security Safeguards Principle Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.	High The data controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. (See Art. 17) Where data processing is carried out by a third party for the data controller, the data controller must obtain guarantees relating to technical and organizational security measures. The third party must be governed by a contract imposing a duty to take security measures and obey the data controller.	Medium A business which collects, holds, uses or communicates personal information about other persons must establish "such safety measures as are appropriate to ensure the confidentiality of the information." (s. 10)	Medium 542 "Banks will protect personal information with safeguards appropriate to the sensitivity of the information." (Pr. 7) Information may be disclosed to third parties for printing cheques, data processing, collection services, or other goods or services. However, banks will require third parties to safeguard information. (Pr. 7.5)	Medium "Personal information will be considered confidential, and comprehensive safeguards will be established by the company to protect that confidentiality." Agents, brokers, plan sponsors and other persons or organizations acting for or on behalf of the company will be required to comply with the Guidelines. (s.9)	Medium "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information." (4.7)
11. OECD Openness principle There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.	High Member states shall take measures to ensure that processing operations are publicized. In particular, member states shall provide that a register of processing operations is kept. The register shall be open to public inspection. (Art. 21) As well, the data controller must notify the supervisory authority established by the member state before carrying out any wholly or partly automatic processing operation. Specific exemptions to the notice requirement are set out.	Low There are no particular provisions relating to openness, although other duties (such as the duty to provide information on collection or on consulting a credit report) may cover aspects of openness.	Medium "Banks will be open about the policies and procedures they use to manage personal information. Customers will have access to information about these policies and procedures. ..." (Pr.8) Banks will make available copies of their privacy codes on request.	Low "Each company will adopt a general policy of openness about the company's practices and policies with respect to the use and protection of personal information. ..." (s.7) Note, however, that the further elaboration of this principle deals only with the individual's right of access to personal information.	Medium "The P&C insurer shall make readily available to customers specific information about its policies and practices relating to the management of personal information." (4.8) Individuals should be able to obtain information about policies and practices without unreasonable effort.

Characteristic	European Union <i>Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data</i> (1995)	Quebec <i>An Act respecting the protection of personal information in the Private Sector, R.S.Q. P. 39.1</i> (1994)	Canadian Bankers Association <i>Privacy Model Code</i> (1996)	Canadian Life and Health Insurance Association <i>Right to Privacy</i> Guideline No. 96	Insurance Bureau of Canada <i>Model Personal Information Code</i> (1996)
<p>12. OECD Individual Participation Principle</p> <p>An individual should have the right:</p> <p>(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;</p> <p>(b) to have communicated to him, data relating to him i) within a reasonable time; ii) at a charge, if any, that is not excessive; iii) in a reasonable manner; and iv) in a form that is readily intelligible to him;</p> <p>(c) to be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and</p> <p>(d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.</p>	<p>High</p> <p>Rights of access and rectification are set out in the EU Directive, subject to listed exemptions. In addition to rectification, the individual may seek erasure or blocking of the data. The data controller must communicate a rectification to third parties, unless this is impossible or involves disproportionate effort.</p> <p>Access: The data subject has a right to make a request for access at reasonable intervals and without excessive delay or expense. Access should be provided in intelligible form and include any available information about the source of information. Access may be refused in cases involving national security, defence, public security, investigation of offences or professional disciplinary matters, or the protection of the data subject or others.</p> <p>Rectification: In addition to rectification of information, the individual may seek erasure or blocking of data if its processing does not comply with the EU Directive. The data subject may require notification of third parties to whom data have been disclosed of any rectification, erasure or blocking of data, unless this is impossible or involves disproportionate effort. (See Arts. 12-13.)</p>	<p>High</p> <p>Rights of access and rectification are set out in Act subject to stated exemptions.</p> <p>Details: The Act's access and rectification provisions flesh out rights that appear in the Civil Code of Quebec. A business must respond to an access request within 30 days, and failure to respond is a deemed refusal of access. (s.32) Access is to be free of charge, except for a reasonable charge for transcription, reproduction or transmission of information. (s. 33) On obtaining access, an individual may insist that information collected otherwise than according to law be deleted. (s. 28)</p> <p>Access may be denied for a variety of stated reasons, including: a temporary denial by a professional health care enterprise if access would result in serious harm to the individual; denial of information to a person under 14 of information of a medical or social nature, denial where access would hinder an investigation into a crime or offence, denial where access would affect judicial proceedings in which the individual or the business has an interest, and denial where the information would include information about another person and disclosure may seriously harm that other person. (ss. 37-40)</p>	<p>Medium</p> <p>Rights of access and correction are set out in the Code. The list of exemptions is open-ended. A bank is required to communicate a correction to a third party only "if necessary."</p> <p>Access: Access is to be provided to the customer within a reasonable time, and for minimal or no cost. Access may be denied in "specific" cases. Examples of reasons for refusal are: retrieval is too costly, information contains references to other persons, information is subject to solicitor-client privilege, information is proprietary to bank, and information may not legally be disclosed. (Pr.9)</p> <p>Correction: Where a customer shows that information is "inaccurate, incomplete, out of date, or irrelevant," the bank will revise it. The bank will disclose the revised information to third parties who received the old information "if necessary." If a bank refuses a request to revise information, the customer may challenge the bank's decision. The bank should make a record of the challenge and if necessary disclose the challenge to third parties. (ss.6.4 & 6.5)</p>	<p>Low</p> <p>Rights of access and correction are set out in the Guidelines. The list of exemptions is open-ended. The correction right is brief and does not address whether the insurer should communicate a correction to a third party.</p> <p>Details: "(a) Upon appropriate identification and written request satisfactory to the company, an individual will be advised of personal information about him/her retained in the company's records. A company may charge a reasonable administration fee to supply the information. Some medical information may be made available only through the individual's designated physician.</p> <p>"(b) Where information cannot be disclosed to the individual, he/she will be given the reasons for not disclosing the information.</p> <p>"(c) An individual may clarify or correct erroneous personal information retained by the company, incoerred or incomplete information will be amended and differences as to the correctness of the information will be noted." (s. 6)</p> <p>The Notes state that insurers may refuse to release information if "it is inappropriate to do in view of legal considerations" and in cases where information as obtained from a surveillance company.</p>	<p>Medium-to-High</p> <p>Rights of access and correction are set out in the Code. The list of exemptions is open-ended. The Code suggests that mediation before an independent party may be available if access is refused. An insurer is required to communicate a correction to a third party "where appropriate."</p> <p>Access: Access should be provided within a reasonable time, and for minimal or no cost. Exceptions to access should be "limited and specific." Reasons for denying access may include: prohibitive cost, personal information that contains references to other individuals, information that cannot be disclosed for legal, security or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege. The insurer may choose to make sensitive medical information available through a medical practitioner. (s.4.3)</p> <p>Refusal of access: If a request for access is denied, the customer shall be given information on how to challenge the denial, including: an invitation to send a letter to the insurer's president, a commitment by the insurer to open a dialogue with the customer, and a commitment by the insurer to participate in an independent mediation process if the parties cannot resolve the dispute, with the Insurance Bureau of Canada assisting in arranging the independent mediation. (s.4.9.1)</p> <p>Correction: If the customer shows that information is inaccurate or incomplete, the insurer must amend the information. Where "appropriate," the amended information shall be transmitted to third parties with access. When a challenge is not resolved to the satisfaction of the customer, the substance of the challenge should be recorded and, where appropriate, the existence of the challenge should be made known to third parties. (ss.4.9.5 & 4.9.6)</p>

Characteristic	European Union <i>Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data</i> (1995)	Quebec <i>An Act respecting the protection of personal information in the Private Sector</i> , R.S.Q. P. 39.1 (1994)	Canadian Bankers Association <i>Privacy Model Code</i> (1996)	Canadian Life and Health Insurance Association <i>Right to Privacy</i> Guideline No. 96	Insurance Bureau of Canada <i>Model Personal Information Code</i> (1996)
13. OECD Accountability A data controller should be accountable for complying with measures which give effect to the principles stated above.	High There is no particular discussion of the accountability principle, but other provisions deal with aspects of accountability (i.e., duty to inform the individual at time of collection of the data, and the duty to inform the individual of certain information if a credit report is used). Enforcement is through a public body with the power to resolve complaints.	High There is no particular discussion of the accountability principle, but other provisions deal with aspects of accountability (i.e., duty to inform the individual at time of collection of the data, and the duty to inform the individual of certain information if a credit report is used). Enforcement is through a public body with the power to resolve complaints.	Medium The Code includes a general discussion of accountability and internal complaint procedures. An individual unsatisfied with the bank's complaint process may complain to the Canadian Banking Ombudsman. Accountability: "Banks are accountable for all personal information in their control, including any personal information disclosed to third parties for processing. Banks will establish policies and procedures to comply with their own privacy codes, and will designate one or more persons to be accountable for compliance." (Pr. 1) Complaints: Each bank will have policies and procedures to receive, investigate and respond to complaints. A bank will investigate all complaints and if a complaint is justified resolve it. Customers who are not satisfied by the handling of their complaint may contact the Office of the Superintendent of Financial Institutions or Canadian Banking Ombudsman. (Pr. 10)	Low The Guidelines contain brief discussion of accountability and the need to establish internal procedures to handle complaints. Accountability: The Foreword to the Guidelines state that "insurance companies must adhere closely to strict rules governing the protection of the confidential information they hold." Accountability: "In order to ensure compliance with the protection of privacy guidelines each company will: (a) designate an officer to receive complaints; (b) establish procedures for receiving and resolving complaints. Individuals dissatisfied with the complaint resolution of a company can contract the office of the insurance regulators in their province." (s.8)	Low-to-Medium The Code includes a general discussion of accountability and internal complaint procedures. The Code raises the possibility of mediation before an independent mediator in the case of a denial of access. Accountability: "The P&C insurer is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the P&C insurer's compliance with the following principles:" (s.4.1) Complaints: The P&C insurer shall have procedures to respond to complaints. The insurer shall investigate all complaints and if a complaint is justified resolve it. Consumers shall be informed of their right to lodge complaints. For example, unsatisfied customers may be able to complain to regulatory bodies. (See s.4.10 generally.) As well, in the case of denials of access to information, the Code raises the possibility of a mediation before an independent mediator. (s.4.9.1)

Characteristic	European Union <i>Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995)</i>	Quebec <i>An Act respecting the protection of personal information in the Private Sector, R.S.Q. P. 39.1 (1994)</i>	Canadian Bankers Association <i>Privacy Model Code (1996)</i>	Canadian Life and Health Insurance Association <i>Right to Privacy Guideline No. 96</i>	Insurance Bureau of Canada <i>Model Personal Information Code (1998)</i>
14. Specific Provisions on Consent	Low There is no lengthy discussion of consent, but consent is mentioned in provisions permitting use of information for a new purpose.	High There is no lengthy discussion of consent in the Act, but consent is mentioned in provisions permitting use of information for a new purpose. The Act sets a very high standard for the nature of consent. (See above for the definition of consent.)	Medium "Banks will make a reasonable effort to make sure customers understand how the personal information will be used and disclosed by the banks. Banks will get consent from their customers before or when they collect, use or disclose personal information. ... A customer's consent can be expressed, implied, or given through an authorized representative. ... Banks, however, may collect, use, or disclose personal information without the customer's consent for legal, security, or certain processing reasons." (Pr.3) Customers may withdraw consent, subject to contractual restrictions, as long as they give the bank reasonable notice, and the consent does not relate to a credit product where the bank must collect and report information after credit has been granted. A bank may ask for SIN information to match credit bureau records but cannot require this information.	Low The Guidelines do not include a detailed discussion of consent. Consent is mentioned briefly in sections dealing with the collection of information and the use or disclosure of information.	Medium "The knowledge and consent of the customer are required for the collection, use or disclosure of personal information, except where inappropriate." (s.4.3) Information may be collected, used or disclosed without knowledge or consent of the customer in situations such as those involving legal, medical or security reasons. Where there is no direct relationship with the customer (i.e., the individual is served by an independent broker or agent) the P&C insurer may not be able to seek consent. However, if certain types of information are being collected – such as medical or hospital records, employment records or tax records – the P&C insurer will obtain express consent from the customer. Consent may be withdrawn subject to contractual restrictions and the requirement that insurers maintain the integrity of necessary statistics and data.

Characteristic	European Union <i>Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995)</i>	Quebec <i>An Act respecting the protection of personal information in the Private Sector, R.S.Q. P. 39.1 (1994)</i>	Canadian Bankers Association <i>Privacy Model Code (1996)</i>	Canadian Life and Health Insurance Association <i>Right to Privacy Guideline No. 96</i>	Insurance Bureau of Canada <i>Model Personal Information Code (1996)</i>
15. Provisions Restricting Transfer Outside the Jurisdiction	<p>Yes</p> <p>Article 25 provides that transfers of data for processing may take place only if the recipient country provides an "adequate" level of protection. Adequacy shall be assessed in light of all the circumstances surrounding the proposed transfer. "[p]articular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and the country of final destination, the rules of law, both general and sectoral, in force in the third country in question, and the professional rules and security measures that are complied with in that country."</p> <p>Article 26 provides some exceptions to Article 25. For example, a transfer may be permitted despite Article 25 if: the data subject has consented, the transfer is necessary for the performance of a contract with the data subject, the transfer is necessary for the performance of a contract in the interest of the data subject, or the transfer is necessary or legally required on important public interest grounds. The transfer is also possible where the data controller ensures special safeguards through, for example, contractual measures.</p>	<p>Yes</p> <p>Before a business within Quebec communicates information relating to Quebec residents to a person outside Quebec, the business must take "all reasonable steps" to ensure that: (1) the information will not be used for purposes not relevant to the file or communicated without consent of the individual except as permitted by the Act's exceptions; and (2) the Act's provisions on the removal of names from nominative lists will be followed. (s.17)</p>	No	No	No

Characteristic	European Union <i>Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data</i> (1995)	Quebec <i>An Act respecting the protection of personal information in the Private Sector, R.S.Q. P. 39.1</i> (1994)	Canadian Bankers Association <i>Privacy Model Code</i> (1996)	Canadian Life and Health Insurance Association <i>Right to Privacy</i> Guideline No. 96	Insurance Bureau of Canada <i>Model Personal Information Code</i> (1996)
<p>16. Special Features of Interest</p>	<p>Yes</p> <p>There are special measures that relate to the processing of personal data, the processing of sensitive data, and automated decision-making.</p> <p>Processing Generally: The EU Directive prohibits the processing of personal data unless one of six exceptions are met. The exceptions are that the data subject has consented to the processing; it is necessary for the performance of a contract, for compliance with a legal obligation; to protect the vital interests of the data subject, for the performance of a task in the public interest, or for purposes of legitimate interests of the data controller. (See Art. 7.)</p> <p>Processing of Sensitive Data: The EU Directive generally prohibits the processing of certain sensitive types of personal data – i.e., data “revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, trade-union membership,” or data “concerning health or sex life.” There are, however, a number of exceptions to this general prohibition. (See Art. 8.)</p> <p>Automated Decision-making: The EU Directive sets out a special right for a person not to be subject to certain types of automated decision-making. Every person “shall not be subject to a decision which produces legal effects and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.” However, the EU Directive permits such decision-making under a contract or under the national law if certain conditions are met. (See Art. 15.)</p>	<p>Yes</p> <p>There are special measures that relate to “nominative lists,” which are defined as lists of “names, addresses or telephone numbers of natural persons.” (s.22)</p> <p>Nominative Lists: Nominative lists may be transferred to a third party only if certain exceptions are met, which include the requirement that before transfer each individual named on the list is given a “valid opportunity” to have his or her name removed from the list (s.22). A business may use a nominative list of its employees or members for commercial or philanthropic prospection. However, each person named on the list must have a “valid opportunity” to have his or her name removed. (s. 23) A business which uses a nominative list for commercial or philanthropic prospection by mail or telephone must identify itself and inform the individual of the right to have his or her name and information deleted from the list. (s. 24) The individual may make a request to have his or her name removed from a list in writing or orally, and the name must then be removed with due diligence. (ss. 25 & 26)</p>	<p>No</p>	<p>No</p>	<p>No</p>

Detailed Comparison Chart (TCAC, CUCC, CSA, U.K., N.Z.)

Characteristic	Trust Companies Association of Canada Customer Privacy Code (1993)	Credit Union Central of Canada <i>Credit Union Code for the Protection of Personal Information, Draft (1996)</i>	Canadian Standards Association <i>Model Code for the Protection of Personal Information (1996)</i>	The United Kingdom <i>Data Protection Act 1984 (c. 35)</i>	New Zealand <i>Privacy Act 1993</i>
1. Type of Document	Model code for trust companies, based on the OECD principles. The TCAC Code is organized according to the OECD principles, with subsections that provide further discussion.	Draft model code for credit unions, based on the CSA Model Code. The CUA Code comes in the form of principles with subpoints that provide further discussion.	Model code for use by a business, to be adapted to the particular circumstances of the business' industry. The CSA Code comes in the form of a set of principles with subpoints that provide further discussion.	Legislation, based on the OECD principles, which regulates the use of automatically processed data.	Privacy legislation in New Zealand, based on OECD principles.
2. Application	Trust companies that adopt the Code.	Credit unions that adopt the Code.	Businesses that adopt the Code.	Public & private sector The Act applies to both the private and public sector with respect to the automatic processing of information but does not regulate information contained in manual records.	Public & private sector The Act applies to every person or organization in New Zealand in respect of personal information held in any capacity other than for the purposes of their personal, family or household affairs.
3. Enforcement	Low Enforcement is by privacy policies and complaint procedures established by trust companies.	Low-to-Medium Enforcement is by privacy policies and complaint procedures established by credit unions. The Code states that if an individual's complaint is not resolved within the credit union, procedures should exist to refer it to Credit Union Central or an independent mediator or arbitrator.	Low Enforcement is by privacy policies and complaint procedures established by adopting businesses. The Code also states that businesses should inform customers of relevant complaint mechanisms, including regulatory bodies which accept complaints.	High The Data Protection Registrar is charged with enforcing the Act and promoting compliance with the Principles. Court action is also available in certain circumstances.	High Enforcement of the Act's provisions is by the Privacy Commissioner, although the Proceedings Commissioner and the Complaints Review Tribunal may make orders for damages or may restrain certain actions. Each organization or agency must designate at least one privacy officer, whose role is to encourage compliance with the privacy principles and the Act. (s. 23)
4. Personal information defined	Yes "[P]ersonal information means data that identify and relate to a specific individual. It includes but is not limited to an individual's name, address, age, identification numbers, assets, liabilities, income, names of third parties to whom information was disclosed, whether or not credit was extended, payment records." (s.2(2))	Yes "[I]nformation about an identifiable individual that is recorded in any form." (Definitions)	Yes "[I]nformation about an identifiable individual that is recorded in any form." (s.2.1)	Yes "Personal data' means data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user), including any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual." (s. 1)	Yes "Personal information' means information about an identifiable individual; and includes information contained in any register of deaths kept under the Births and Deaths Registration Act 1951." (s. 2)

Characteristic	Trust Companies Association of Canada Customer Privacy Code (1993)	Credit Union Central of Canada <i>Credit Union Code for the Protection of Personal Information, Draft (1996)</i>	Canadian Standards Association <i>Model Code for the Protection of Personal Information (1996)</i>	The United Kingdom <i>Data Protection Act 1984 (c. 35)</i>	New Zealand <i>Privacy Act 1993</i>
5. Consent defined	No	Yes "I]voluntary agreement with what is being done or proposed. Consent can be either express or implicit. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the credit union seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the member." (Definitions)	Yes "I]voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, whether orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual." (s.2.1)	No	No

Characteristic	Trust Companies Association of Canada Customer Privacy Code (1993)	Credit Union Central of Canada Credit Union Code for the Protection of Personal Information, Draft (1996)	Canadian Standards Association Model Code for the Protection of Personal Information (1996)	The United Kingdom Data Protection Act 1984 (c. 35)	New Zealand Privacy Act 1993
<p>6. OECD Collection Limitation Principle</p> <p>There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.</p>	<p>Medium</p> <p>"Member trust companies collect only that personal information about their customers needed for the purposes specified in section 6(2) of this Code. ..."</p> <p>(s.4(1)) Section 6(2) provides the following purposes: to establish or maintain relationships with customers; to offer and provide products and services as permitted by law; to comply with the law; and to protect the interests of the customer and the trust company. Trust companies will collect personal information only by lawful means.</p>	<p>Low-to-Medium</p> <p>"The collection of personal information will be limited to that which is necessary for the purposes identified by the credit union. Information will be collected by fair and lawful means." (Pr.4.0) Credit unions will collect information: to aid in understanding the member's needs; to determine the suitability of the products and services for the member or the eligibility of the member; to set up, offer and manage products and services that meet the member's needs; to provide ongoing service; to meet legal and regulatory requirements. (s.2.2)</p>	<p>Low-to-Medium</p> <p>"Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means." (Pr.4) Businesses shall not collect information indiscriminately. The amount and type of information shall be limited to that which is necessary to fulfil the purposes identified.</p>	<p>Medium-to-High</p> <p>The data user can only obtain or hold personal data that complies with the data Registrar upon registration, (ss.4-5) "The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully." (Principle 1) In determining whether the information was obtained fairly, "regard shall be had to the method by which it was obtained, including in particular whether any person from whom it was obtained was deceived or misled as to the purpose or purposes for which it is to be held, used or disclosed." (Interpretation of Pr. 1)</p>	<p>Medium-to-High</p> <p>Information Privacy Principles 2 to 4 limit or restrict the collection of personal information by agencies (that is, any person, company or Government department) "Where an agency collects personal information, the agency shall collect the information directly from the individual concerned." (Pr. 2) Personal information is not to be collected by unlawful means or by means which are unfair or unreasonably intrusive. (Pr. 4)</p>
<p>7. OECD Data Quality Principle</p> <p>Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.</p>	<p>Medium-to-High</p> <p>"To the best of their abilities, member trust companies will ensure that the personal information they keep about their customers is as accurate, as complete as is required, for the purpose, and as up-to-date as possible. ..."</p>	<p>Medium</p> <p>"Personal information will be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used." (Pr.6.0) The extent to which information must meet this standard will depend on the use of the information, taking into account the interests of the member. Information should be sufficiently accurate, complete and up-to-date to "minimize the possibility" of inappropriate information may be used to make a decision.</p>	<p>Medium</p> <p>"Accuracy: Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used." (Pr.6) The extent to which information must meet this standard will depend on the use of the information, taking into account the interests of the individual. Information should be sufficiently accurate, complete and up-to-date to "minimize the possibility" of inappropriate information may be used to make a decision.</p>	<p>High</p> <p>"Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes." (Pr. 4) "Personal data shall be accurate and, where necessary, kept up to date." (Pr. 5) The data is not to be "kept for longer than is necessary." (Pr. 6)</p>	<p>High</p> <p>"An agency that holds information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading." (Pr. 8) "An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used." (Pr. 9)</p>

Characteristic	Trust Companies Association of Canada Customer Privacy Code (1993)	Credit Union Central of Canada <i>Credit Union Code for the Protection of Personal Information, Draft</i> (1996)	Canadian Standards Association <i>Model Code for the Protection of Personal Information</i> (1996)	The United Kingdom <i>Data Protection Act</i> 1984 (c. 35)	New Zealand <i>Privacy Act</i> 1993
<p>8. OECD Purpose Specification Principle</p> <p>The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.</p>	<p>Low</p> <p>"Before or at the time of collection, member trust companies advise their customers of the purposes for which the personal information is collected." (s. 3(1)) Trust companies will collect personal information primarily from customers, but also from external sources such as credit grantors, credit bureaus, income sources, and personal references. Trust companies will obtain the consent before verifying and supplementing information with external sources. (s.4)</p>	<p>Low</p> <p>"The purposes for which personal information is collected will be identified by the credit union when collected." (Pr.2.0) The identified purposes should be specific to the member from whom information is being collected. When personal information is to be used for a purpose other than the purpose for which it was collected, the consent of the member will be required unless the new purpose is required by law.</p>	<p>Low</p> <p>Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected." (Pr.2) When personal information is to be used for a new purpose not previously identified, the new purpose shall be identified before use. Unless the new purpose is required by law, the consent of the individual must be obtained before the information can be used for the new purpose.</p>	<p>High</p> <p>Upon registering, the data user must provide, among other things, a description of: (1) the personal data to be held and the purposes for which such data will be held or used; (2) the source from which the data will be obtained; (3) any person to whom the data may be disclosed; and (4) any countries outside of the UK to which the data may be directly or indirectly transferred. (s. 4) The data user must apply to the Registrar to make any alterations to the above description. (s. 6) Furthermore, Personal data is to "be held only for one or more specified and lawful purposes." (Pr. 2)</p>	<p>Medium-to-High</p> <p>The agency must take reasonable steps to ensure that the individual from whom information is being collected is aware of, among other things, the fact that the information is being collected, the purpose for which it is being collected and the intended recipients of the information. This should be explained before the information is collected or as soon as practicable. (Pr. 3). Personal information is not to be collected by any agency unless the information is collected for a lawful purpose and is necessary for that purpose. (Pr. 1)</p>

Characteristic	Trust Companies Association of Canada Customer Privacy Code (1993)	Credit Union Central of Canada Credit Union Code for the Protection of Personal Information, Draft (1996)	Canadian Standards Association Model Code for the Protection of Personal Information (1996)	The United Kingdom Data Protection Act 1984 (c. 35)	New Zealand Privacy Act 1993
<p>9. OECD Use Limitation Principle</p> <p>Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the purpose specification principle] except: (a) with the consent of the data subject; or (b) by the authority of law.</p>	<p>Medium</p> <p>"Before member trust companies use personal information for purposes other than those for which it was collected or for such others that are compatible with those purposes, they will obtain their customers' consent." (s. 7(1))</p> <p>Trust companies will disclose personal information to third parties only if one of four exceptions applies: the customer has consented, the trust company is under the legal obligation to do so, the trust company has a public duty to do so, or the trust company is required to do so to protect its own interests. (s.7(2)) The Code notes that exchange of personal information with third parties such as credit grantors and credit bureaux requires customer consent unless permitted by the Code.</p>	<p>Medium</p> <p>"Personal information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the member or as required by law. Personal information will be retained only as long as necessary for the fulfillment of those purposes."</p> <p>The credit union may disclose personal information without consent where required by law, such as in the case of a subpoena, search warrant, other court or government order, or demands from parties with a legal right to personal information.</p> <p>A member's health records may be used for credit application and related insurance purposes. The health records will not be collected from or disclosed to any other organization.</p>	<p>Medium</p> <p>"Limiting Use, Disclosure and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as is necessary for the fulfillment of those purposes." (Pr.5)</p>	<p>High</p> <p>A data user cannot hold any data for any purpose other than the purpose(s) described in the register entry nor disclose any data held to any person not described in the entry (s. 5) "Personal data purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes." (Pr. 3)</p>	<p>Medium</p> <p>"An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose...." barring certain exceptions. An agency may use personal information for another purpose if, for example, it believes that it is a directly related purpose, that the source of information is a publicly available document, or that the information is used in a form in which the individual concerned is not identified. (Pr. 10) An agency may not disclose personal information unless it reasonably believes, among other things, that the "disclosure of the information is one of the purposes for directly related to the purposes] in connection with which the information was obtained." (Pr. 11)</p>
<p>10. OECD Security Safeguards Principle</p> <p>Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.</p>	<p>Medium</p> <p>"Member trust companies implement comprehensive security measures to protect personal information against loss or unauthorized access, use, disclosure, modification or destruction." (s.8(1))</p> <p>Information may be disclosed to businesses such as cheque printers, data processors or mailing service agencies and collection agencies, which will be required to treat the information as confidential. (s. 8(3))</p>	<p>Medium</p> <p>"Personal information will be protected by security safeguards appropriate to the sensitivity of the information." (Pr.7.0)</p> <p>Third parties (such as cheque printers, data processors, credit collection agencies and credit bureaux) will be required to safeguard personal information disclosed to them in a manner consistent with the policies of the credit union.</p>	<p>Medium</p> <p>"Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information." (Pr.7)</p>	<p>Medium</p> <p>"Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data." (Pr. 8)</p>	<p>Medium</p> <p>An agency that holds personal information must ensure that the information is protected by reasonable security safeguards against loss, misuse, or unauthorized access, use, modification, or disclosure. Where it is necessary for the information to be given to a person in connection with the provision of a service, "everything reasonably within the power of the agency [must be] done to prevent unauthorized use or unauthorized disclosure of the information." (Pr. 5)</p>

Characteristic	Trust Companies Association of Canada Customer Privacy Code (1993)	Credit Union Central of Canada <i>Credit Union Code for the Protection of Personal Information, Draft (1996)</i>	Canadian Standards Association <i>Model Code for the Protection of Personal Information (1996)</i>	The United Kingdom <i>Data Protection Act 1984 (c. 35)</i>	New Zealand <i>Privacy Act 1993</i>
11. OECD Openness principle There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.	Low "Member trust companies are open about their policies on the protection of the confidentiality of customer personal information. Questions and concerns about an individual company's policies should be directed to the individual company." (s.2(1))	Medium "The credit union will make readily available to members specific, understandable information about its policies and practices relating to the management of personal information." Information will be readily available in a form that is generally understandable. (Pr.8.0)	Medium "Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information." (Pr. 8) Individuals should be able to acquire information about a business' policies and practices without unreasonable effort.	High A data user is not entitled to hold personal data unless he registers with the Registrar as a data user or computer bureau. The entries in the register are to be made available for public inspection. (s. 9) One of the duties of the Registrar is to inform the public about the operation of the Act. (s. 36)	High In addition to the general duty of the Privacy Commissioner to promote an understanding of the privacy principles, the Commissioner may also publish certain publications which may include such information as the nature of personal information held by any agency, the purpose and length of time for which it is held, the individuals who are entitled to have access to the personal information held by an agency and the steps to be taken to obtain access. (s. 21) The Commissioner may require an agency to supply information for the purpose of these publications. (s. 22)

Characteristic	Trust Companies Association of Canada Customer Privacy Code (1993)	Credit Union Central of Canada Protection of Personal Information, Draft (1996)	Canadian Standards Association Model Code for the Protection of Personal Information (1996)	The United Kingdom Data Protection Act 1984 (c. 35)	New Zealand Privacy Act 1993
12. OECD Individual Participation Principle <i>An individual should have the right</i>	<p>Medium</p> <p>Rights of access and correction are set out in the Code. The access right is restricted in that it does not apply to opinion and judgments about the individual. The list of exemptions is open-ended. However, the trust company must use its "best efforts" to communicate a correction to a third party if prior incorrect information may result in the customer's interests being harmed.</p> <p>Access: Customers have the right to have access to information about them held by a trust company, except for opinions and judgments. The trust company will provide access within a reasonable time, at a reasonable cost. Access will be given unless there is a "valid" reason for refusing to do so.</p> <p>Correction: Customers may challenge incorrect, incomplete or redundant information. Incorrect or incomplete information will be amended, and superfluous information will be deleted. Differences as to correctness or completeness will be noted. If a trust company has disclosed incorrect information to a third party, and this information may result in the customer's interests being harmed, the trust company will use its best efforts to communicate the corrected information to the third party.</p>	<p>Medium</p> <p>Rights of access and correction are set out in the Code. The list of exemptions is open-ended. A credit union is required to communicate a correction to a third party "where appropriate."</p> <p>Access: Access should be provided within a reasonable time, for no cost or a reasonable cost. Exceptions to access should be "limited and specific." Reasons for denying access may include: prohibitive cost, personal information that contains references to other individuals, information that cannot be disclosed for legal, security or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege. The credit union may choose to make sensitive medical information available through a medical practitioner.</p> <p>(Pr.9, ss.9.1 & 9.2.)</p> <p>Correction: If the member demonstrates that information is inaccurate or incomplete, the credit union must amend the information. Where "appropriate," the amended information shall be transmitted to third parties having access to the information. When a challenge is not resolved to the satisfaction of the member, the substance of the unresolved challenge should be recorded. Where "appropriate" the existence of the challenge should be transferred to third parties having access to the information.</p> <p>(ss.9.6 & 9.7)</p>	<p>Medium</p> <p>Rights of access and correction are set out in the Code. The list of exemptions is open-ended. A business should communicate a correction to a third party "where appropriate."</p> <p>Access: Access should be provided within a reasonable time, and at minimal or no cost to the individual. Exceptions to access should be "limited and specific." Reasons for denying access may include: prohibitive cost, personal information that contains references to other individuals, information that cannot be disclosed for legal, security or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege. The business may choose to make sensitive medical information available through a medical practitioner. (ss.4.9.1-4.9.4)</p> <p>Correction: If the individual demonstrates that information is inaccurate or incomplete, the business must amend the information. Where "appropriate," the amended information shall be transmitted to third parties having access to the information. When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge should be recorded. Where "appropriate" the existence of the challenge should be transferred to third parties having access to the information. (ss.4.9.5 & 4.9.6)</p>	<p>High</p> <p>Rights of access and correction are set out in the Act, subject to listed exemptions.</p> <p>"An individual shall be entitled (a) at reasonable intervals and without undue delay or expense (i) to be informed by any data user whether he holds personal data of which and (ii) to access any such data held by a data user; and (b) where appropriate, to have such data corrected or erased." (Pr. 7)</p> <p>Upon the data subject making a written request, accompanied by a fee, the data user must supply the information with a copy of the information within 40 days. (s. 21) An individual is entitled to compensation for any damage or distress suffered as a result of the inaccuracy, loss, unauthorized disclosure or unauthorized disclosure of data held by a data user. (ss. 22-23) A court may also, upon application and subject to certain conditions, order the rectification or erasure of any data held by a data user. (s. 24)</p>	<p>High</p> <p>Rights of access and rectification are set out in Act subject to stated exemptions.</p> <p>Access</p> <p>An individual is entitled to obtain confirmation from an agency as to whether it holds personal information on him and if so, is entitled to have access to that information. (Pr. 6) If the agency does not hold the requested information but believes another agency does, it must transfer the request within 10 days. (s. 39) The agency must respond within 20 working days as to whether it will comply with the request unless an extension is requested (ss. 40-41). If the agency refuses the request, it must state the reason for its refusal and give the individual information concerning his right to seek an investigation and review of the refusal. (s. 44)</p> <p>Rectification</p> <p>An individual is entitled to request correction of personal information held by an agency or an attachment to the information was sought but not made. An agency which holds personal information must take reasonable steps, either on its own initiative or at the request of the individual concerned, to ensure that the information is "accurate, up to date, complete, and not misleading." (Pr. 7) An individual who is making a request relating to the access or correction of information held in a document is to be given either a copy of the document or a reasonable opportunity to inspect it. (s. 42)</p>

Characteristic	Trust Companies Association of Canada Customer Privacy Code (1993)	Credit Union Central of Canada <i>Credit Union Code for the Protection of Personal Information, Draft (1996)</i>	Canadian Standards Association <i>Model Code for the Protection of Personal Information (1996)</i>	The United Kingdom <i>Data Protection Act 1984 (c. 35)</i>	New Zealand <i>Privacy Act 1993</i>
<p>13. OECD Accountability Principle</p> <p>A data controller should be accountable for complying with measures which give effect to the principles stated above.</p>	<p>Low</p> <p>The Code includes brief discussion of accountability and internal complaint procedures.</p> <p>Accountability: "Senior management within each trust company is responsible for ensuring compliance with the provisions of this Code and for ensuring that customer complaints are addressed. However, day-to-day implementation of privacy procedures can be assigned to specific staff members." (s.10(1))</p> <p>Complaints: Trust companies will have clear and timely procedures for dealing with customer complaints. Customers dissatisfied with the company's complaints process may contact the Office of the Superintendent of Financial Institutions. (s.10)</p>	<p>Low-to-Medium</p> <p>The Code includes a general discussion of accountability and internal complaint procedures. It suggests that complaints not resolved internally should be referred to the Credit Union Central or an independent mediator or arbitrator.</p> <p>Accountability: "The credit union is responsible for personal information under its control and will designate an individual who is accountable for the credit union's compliance with the principles of the Code." (Pr. 1.0)</p> <p>Complaints: Each credit union will have policies and procedures to receive and respond to complaints. A credit union will investigate all complaints and if a complaint is justified take appropriate measures. If the complaint is not satisfactory resolved by the designated credit union official, it may be taken to the credit union board of directors. If the complaint is not resolved by the board, there should be procedures to refer the complaint to the Credit Union Central, to a regulator or to an independent mediator or arbitrator. (Pr. 10)</p>	<p>Low</p> <p>The Code includes a general discussion of accountability and the need for internal complaint procedures. It also suggests that individuals should be informed of the existence of regulators who may accept complaints.</p> <p>"Accountability: An organization is responsible for personal information under its control, and shall designate an individual or individuals who are accountable for the organization's compliance with the Code's principles." (Pr. 1)</p> <p>"Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance." (Pr. 10)</p> <p>Businesses should inform individuals about the existence of relevant complaint mechanisms, including regulatory bodies that accept complaints. A business shall investigate all complaints and if a complaint is found to be justified take appropriate measures.</p>	<p>High</p> <p>There is no particular discussion of the accountability principle, but other provisions deal with aspects of accountability (i.e., the appointment of privacy officers, the duty to inform the individual at the time of collection of the data, the publication of information held by agencies, the regulatory status of codes of practice adopted by agencies). Enforcement is through public authorities.</p>	<p>High</p> <p>There is no particular discussion of the accountability principle, but various provisions deal with aspects of accountability (i.e., the appointment of privacy officers, the duty to inform the individual at the time of collection of the data, the publication of information held by agencies, the regulatory status of codes of practice adopted by agencies). Enforcement is through public authorities.</p>

Characteristic	Trust Companies Association of Canada Customer Privacy Code (1993)	Credit Union Central of Canada <i>Credit Union Code for the Protection of Personal Information, Draft (1996)</i>	Canadian Standards Association <i>Model Code for the Protection of Personal Information (1996)</i>	The United Kingdom <i>Data Protection Act 1984 (c. 35)</i>	New Zealand <i>Privacy Act 1993</i>
14. Specific Provisions on Consent	Low The Code does not include a detailed discussion of consent. Consent is mentioned briefly in sections dealing with the collection of information and the use or disclosure of information.	Medium "The knowledge and consent of the member are required for the collection, use, or disclosure of personal information, except where inappropriate." (Pr. 3) Information may be collected, used or disclosed without knowledge or consent of the customer in situations such as those involving legal, medical or security reasons. In determining the form of consent to use, the credit union will take into account the sensitivity of the information. The reasonable expectations of the member are relevant when determining when consent must be obtained. A member may withdraw consent at any time, subject to legal or contractual restrictions, provided that reasonable notice is given, and consent does not relate to a credit product requiring the collection and reporting of information after the credit has been granted.	Medium "Consent: The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate." (Pr. 3) Information may be collected, used or disclosed without knowledge or consent of the customer in situations such as those involving legal, medical or security reasons. Organizations without a direct relationship may not be able to seek consent. In determining the form of consent to use, the business will take into account the sensitivity of the information. The reasonable expectations of the member are relevant when determining when consent must be obtained. An individual may withdraw consent at any time, subject to legal or contractual notice and reasonable notice.	Low Consent of a data subject is not dealt with in the Act.	Low There is little discussion of consent; consent is mentioned in provisions which limit the use and disclosure of personal information.

Characteristic	Trust Companies Association of Canada Customer Privacy Code (1993)	Credit Union Central of Canada <i>Credit Union Code for the Protection of Personal Information, Draft (1996)</i>	Canadian Standards Association <i>Model Code for the Protection of Personal Information (1996)</i>	The United Kingdom <i>Data Protection Act 1984 (c. 35)</i>	New Zealand <i>Privacy Act 1993</i>
15. Provisions Restricting Transfer Outside the Jurisdiction	No	No	No	Yes The Registrar may serve a transfer prohibition notice on a data user prohibiting the user from transferring data outside of the United Kingdom on a permanent basis or until such steps are taken as to ensure the protection of the interests of the data subjects. When transfers of data are to states not bound by the European Convention, the Registrar must be satisfied that the transfer is likely to contravene any of the data protection principles before serving the prohibition notice. When transfers of data are to states bound by the European Convention, notice will not be served unless the Registrar is satisfied that a further transfer to a state not bound by the Convention is likely to lead to a contravention of the data protection principles. (s. 12)	No The Act does not specifically refer to transborder data flows, but relies upon the relevant information privacy principles to govern such transfers.

Characteristic	Trust Companies Association of Canada Customer Privacy Code (1993)	Credit Union Central of Canada <i>Credit Union Code for the Protection of Personal Information, Draft (1996)</i>	Canadian Standards Association <i>Model Code for the Protection of Personal Information (1996)</i>	The United Kingdom <i>Data Protection Act 1984 (c. 35)</i>	New Zealand <i>Privacy Act 1983</i>
16. Special Features of Interest	No	No	No	<p>Yes</p> <p>Processing of Sensitive Data:</p> <p>The Act states that the data protection principles may be modified or supplemented by the Secretary of the State in order to provide additional safeguards with respect to personal data consisting of information as to the data subject's racial origin, political opinions or religious or other beliefs, physical or mental health or sexual life, or his criminal convictions. (s. 2)</p> <p>Note: The UK is in the process of introducing a new data protection bill which will implement the 1995 EU Data Protection Directive. The bill has received its first reading in the House of Lords and the second reading is expected to occur in February, 1998. The new scheme will simplify the notification and registration requirements. Unlike the current Act, it will also apply to non-automated records. The new law will enable individuals who believe their privacy rights have been breached to seek redress in the courts, in addition to taking their complaints before the supervisory authority. The new legislation will include provisions on automated decision making, on consent, on criteria to be met before processing may begin, especially in the case of sensitive data, and on circumstances in which transfers of personal data to countries with 'inadequate protection' may occur.</p>	<p>Yes</p> <p>There are special provisions relating to unique identifiers, codes of practice, information matching, and public register privacy principles.</p> <p>Unique Identifiers</p> <p>An agency is not allowed to assign a unique identifier to an individual unless such as assignment is necessary to enable the agency to carry out its functions efficiently. Once an identifier is assigned by one agency, it cannot be used by any other unassociated agency. (Pr. 12)</p> <p>Codes of Practice</p> <p>Codes of practice may, after public notice and consultation, be initiated by the Commissioner or any agency and are enforceable, legally-binding documents under the Act. A code of practice may modify one or more of the information privacy principles. (Part VI, ss. 46-57)</p> <p>Information Matching</p> <p>The Act limits matching programs to a few "specified" public agencies, which are required to sign information matching agreements which impose controls upon the disclosure of information. An "unspecified" agency is not entitled to participate in a matching program unless certain objectives are met. (Part X, ss. 97-109)</p> <p>Public Register Privacy Principles</p> <p>The Act sets out 4 principles dealing with public registers. Government departments which administer the public registers must comply with the information and public register privacy principles in the absence of other overriding statutes. (Part VII, ss. 58-65)</p>

Table of Cases

Cases	Page
<i>A.-G. Ontario v. A.-G. Canada</i> [1896] A.C. 348 (P.C.)	124
<i>A.-G. Ontario v. A.-G. Canada</i> [1937] A.C.405 (P.C.)	122
<i>A.-G. Ontario v. Canada Temperance Foundation</i> [1946] A.C. 193 (P.C.)	124
<i>Allan Mather v. Columbia House</i> , an unreported case decided August 6, 1992 by the Ontario Court (General Division)	44
<i>Anti-Inflation Act</i> [1976] 2 S.C.R. 373	124
<i>Australian Securities Commission v. Westpac Banking Corporation</i> (1991), A.C.S.R. 350, 32 F.C.R. 546	53
<i>Bank of Tokyo Ltd. v. Karoon</i> [1987] A.C. 45, [1986] 3 All E.R. 468 (C.A.)	53
<i>Banks v. Biensch</i> (1977), 5 A.R. 83 (S.C.)	57
<i>Bernstein of Leigh v. Skyviews & General Ltd.</i> , [1978] 1 Q.B. 479	44
<i>Bhogal v. Punjab National Bank</i> , [1988] 2 All E.R. 296 (C.A.)	53
<i>Budzich v. Toronto Dominion Bank</i> , [1996] 2 C.T.C. 278	54
<i>Burrows v. Superior Court of San Bernardino County</i> (1974), 13 Cal. 3d 238, 118 Cal. Rptr. 166, 529 P.2d 590	53
<i>Cambridge Water Company v. Eastern Counties Leather</i> , [1994] 1 All E.R. 53	46
<i>Canada Deposit Insurance Corp. v. Canadian Commercial Bank</i> (1989), 64 Alta. L.R. (2d) 329, 71 C.B.R. (N.S.) 239, 95 A.R. 24, A.W.L.D. 367	54
<i>Canadian Imperial Bank of Commerce v. Sayani</i> , (1993), 83 B.C.L.R. (2d)167	55
<i>CIBC v. A.-G. Can.</i> (1962), 35 D.L.R. (2d) 49 (S.C.C.)	53
<i>Citizens' Insurance Co. v. Parsons</i> (1881), 7 App. Cas. 96 (P.C.)	122
<i>Cossette v. Dun</i> (1891), 18 S.C.R. 22	45
<i>Dominion Stores v. The Queen</i> , [1980] 1 S.C.R. 844	122
<i>Duchess of Argyll v. Duke of Argyll</i> [1967], Ch.D. 302	47

<i>Farm Products Marketing Act</i> , [1957] S.C.R. 198	122
<i>Foundation Co. of Canada Ltd. v. Dhillon</i> , [1995] O.J. 3211 (Ont. Ct. Gen. Div.)	54
<i>Frame v. Smith</i> , [1987] 2 S.C.R. 99	47
<i>General Motors v. City National Leasing</i> , [1989] 1 S.C.R. 641	122
<i>Georgia Construction Co. v. Pacific Great Eastern R. Co.</i> , [1929] 4 D.L.R. 161 (S.C.C.)	56, 57
<i>Gillet v. Nissen</i> (1976), 58 D.L.R. (3d) 104 (Alta. S.C.)	45
<i>Grieg v. Grieg</i> , [1966] V.R. 376 (S.C.)	44
<i>Guertin v. Royal Bank of Canada</i> (1983), 43 O.R. (2d) 363	53
<i>Haughton v. Haughton</i> , [1965] 1 O.R. 481	53
<i>Hodge v. The Queen</i> (1883), 9 App. Cas. 117 (P.C.)	121
<i>Hongkong Bank of Canada v. Phillips</i> , [1997] M.J. No. 134 (Man. Q.B.)	53, 55
<i>Hull v. Childs & Huron and Erie Mortgage Corp.</i> , [1951] O.W.N. 116	53
<i>Irwin Toy v. Quebec</i> [1989] 1 S.C.R. 927	121
<i>Jacobsen v. Citizens State Bank</i> (1979), 587 SW2d 480 (Tex. Civ. App.)	53
<i>Johannesson v. West St. Paul</i> , [1952] 1 S.C.R. 292	123
<i>Kabwand Pty. Ltd. v. National Australian Bank Limited</i> (1989), No. G355, Fed. No. 195 (Aust. F.C.)	53
<i>Kingston Thoroughbred Horse Stud and Australian Tax Office No. N85/130</i> (1986), (Administrative Appeals Tribunal)	53
<i>Labatt Breweries v. A-G. Canada</i> , [1980] 1 S.C.R. 844	122
<i>LAC Minerals v. International Corona Resources Ltd.</i> , [1989] 2 S.C.R. 574	46
<i>Libyan Arab Foreign Bank v. Bankers Trust Co.</i> , [1988] 1 Lloyd's Rep. 259	54
<i>MacDonald v. Vapor Canada</i> , [1977] 2 S.C.R. 134	122
<i>Malone v. Commissioner of Police (No. 2)</i> , [1979] 2 All E.R. 620 (Ch.D.)	44
<i>Marcel v. Commissioner of Police of the Metropolis</i> , [1992] 1 All E.R. 72, Ch. 225	54
<i>Midland Doherty Limited v. Rohrer</i> (1984), 62 N.S.R. (2d) 205 (N.S.T.D.)	56

<i>Motherwell v. Motherwell</i> , [1976] 6 W.W.R. 550, 1 A.R. 47, 73 D.L.R. (3d) 62 (C.A.)	44
<i>Munro v. National Capital Commission</i> , [1966] S.C.R. 663	123
<i>Murano v. Bank of Montreal</i> (1995), 31 C.B.R. (3d) 1, 20 B.L.R. (2d) 61	54
<i>Ontario Hydro v. Ontario</i> , [1993] 3 S.C.R. 327	123
<i>Papp v. Papp</i> , [1970] 1 O.R. 331 (Ont. C.A.)	121
<i>Park v. Bank of Montreal</i> , [1997] B.C.J. No. 787	53, 54
<i>Peter Lawrence Crawley et al</i> (1981), 52 F.L.R. 123	53
<i>Pharand Ski Corporation v. Alberta</i> (1991), 7 C.C.L.T. 225 (Alta. Q.B.)	46
<i>Pigg v. Robertson</i> (1977), 549 SW2d 597	53
<i>R. v. Crown Zellerbach</i> , [1988] 1 S.C.R. 401	124
<i>R. v. Duarte</i> (1990), 65 D.L.R. (4th) 240 (S.C.C.)	18
<i>R. v. Lillico</i> , (1994), 92 C.C.C. (3d) 90 (Ont. Ct. Gen. Div.)	54
<i>R. v. Spencer</i> (1983), 2 C.C.C. (3d) 526 (C.A.), per McKinnon A.C.J.O	53
<i>Regulation and Control of Radio Communication in Canada</i> [1932] A.C. 304 (P.C.) at 312	123
<i>Robertson v. Canadian Imperial Bank of Commerce</i> , [1995] 1 All E.R. 824 (P.C.)	53
<i>Royal Bank of Canada v. Art's Welding & Machine Shop</i> (1989), 34 C.P.C. (2d) 190	53, 55
<i>Royal Bank of Canada v. Brattberg</i> (1993), 11 Alta. L.R. (3d) 190, 8 W.W.R. 139, 143 A.R. 131, A.W.L.D. 684	55
<i>Russell v. The Queen</i> (1882), 7 App. Cas. 829 (P.C.)	124
<i>Rylands v. Fletcher</i> , (1866) L.R. 1 Ex 265, aff'd (1868), L.R. 3 H.L. 330	46
<i>Sheen v. Clegg</i> , Unreported. A description of the case appeared in the Daily Telegraph on June 22, 1961	44
<i>Smith v. Kamloops and District Elizabeth Fry Society</i> , [1995] B.C.J. No. 516 (B.C.S.C.), aff'd (1996), 136 D.L.R. (4 th) 644 (C.A.)	57
<i>Smorgen v. Australia and New Zealand Banking Group Ltd</i> (1976), 134 C.L.R. 475	53
<i>State v. McCray</i> , (1976) 15 Wash. App. 810, 551 P.2d 1376	53

<i>Suburban Trust Co.</i> (1979), 408 A.2d 758	53
<i>Sutherland v. Barclays Bank Ltd.</i> (1938), 5 L.D.A.B. 163	55
<i>Taylor v. Commerical Bank</i> (1903), 174 NY 181, 66 NE 726	53
<i>The Queen v. Hauser</i> , [1979] 1 S.C.R. 984	125
<i>Tournier v. National Provincial & Union Bank of England</i> , [1924] 1 K.B. 461 (C.A.)	47
<i>Union Colliery Co. v. Bryden</i> , [1899] A.C. 580 (P.C.)	121
<i>United States Department of Justice v. Reporters Committee for Freedom of the Press</i> (1989), 489 U.S. 749	18
<i>Weld-Blundell v. Stephens</i> , [1920] A.C. 956	54
<i>X A.-G. v. A Bank</i> , [1983] 2 All E.R. 464	54
<i>X. v. Y.</i> , [1988] 2 All E.R. 648	47

Bibliography

Australia, Attorney General's Department, *Privacy Protection in the Private Sector* (September 1996). <http://www.agps.gov.au/customer/agd/clrc/privacy.htm>.

Benn, S.I. *Privacy, Freedom and Respect for Persons* (Lieber-Atherton, 1971).

Burns, P. "The Law and Privacy: The Canadian Experience," (1976) 54 *Canadian Bar Review* 5.

Canadian Bankers Association, *Privacy Model Code: Protecting individual bank customers' privacy* (Toronto: Canadian Bankers Association, 1996).

Canadian Banking Ombudsman, *Report for the nine months ended July 31, 1997* (Toronto: Canadian Banking Ombudsman, 1996).

Canadian Banking Ombudsman, *Annual Report 1996* (Toronto: Canadian Banking Ombudsman, 1996).

The Canadian Institute, *The Internet and Online Services: Exploring the Legal Implications of Doing Business Electronically* (Toronto: The Canadian Institute, March 6&7, 1995).

Carlin, F.M. "The Data Protection Directive: the introduction of common privacy standards," (1996) 21 *European Law Review* 65.

Cate, F.H. "The EU Data Protection Directive, Information Privacy, and the Public Interest," (1995) 80 *Iowa Law Review* 431.

Cavoukian, Ann, *Data Mining: Staking A Claim on Your Privacy* (Ontario: Information and Privacy Commissioner, January 1998).

Consumers' Association of Canada, *Consumer Data Protection* (Ottawa: Consumers' Association of Canada, March 1993).

Consumers' Association of Canada, *Privacy and Data Protection: Background Paper* (Ottawa: Consumers' Association of Canada, July 1992).

Consumers' Association of Canada, *Privacy in the Age of the Information Highway* (Ottawa: Consumers' Association of Canada, March 1995).

Consumers Association of Canada, *Reform of Financial Services: Retailing of Insurance by Deposit-Taking Institutions* (Ottawa: Consumers Association of Canada, August, 1995).

Credit Union Central of Canada, *Credit Union Code for the Protection of Personal Information (Draft)* (Ottawa: Credit Union Central of Canada, 1996).

Downey, Catherine M. "The high price of a cashless society: exchanging privacy rights for digital cash?" (1996) 14 *John Marshall Journal of Computer & Information Law*.

Ekos Research Associates Inc., *Privacy Revealed: The Canadian Privacy Survey* (Ottawa: Ekos Research Associates, 1993).

Estadella-Yuste, Olga, "The Draft Directive of the European Community Regarding the Protection of Personal Data," (1992) 41 *International and Comparative Law Quarterly* 170.

European Commission Directorate General, *First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy: Discussion Document Adopted by the Working Party on June 26, 1997*. <http://www.open.gov.uk.dpr/d5020en2.htm>.

Financial System Inquiry, *Financial System Inquiry Final Report*, Vols. 1, 2 and 3 (Canberra, Australia: Australian Government Publishing Service, 1997).

Fried, C. "Privacy," (1968) 77 *Yale Law Journal* 475.

Gavison, R. "Privacy and the limits of law," (1980) 89 *Yale Law Journal* 42.

Hammond, R.G. "Quantum Physics, Econometric Models and Property Rights to Information," (1981) 27 *McGill Law Journal* 47.

Insight Information Inc. *Electronic Delivery of Financial Services*. (Toronto: Insight Information Inc., 1995).

Insurance Bureau of Canada, *Model Personal Information Code* (Toronto: Insurance Bureau of Canada, 1996).

Lawson, Ian and Woods, David, *Privacy and the Information Highway: Regulatory Options for Canada*. A study prepared for Industry Canada (Ottawa: Industry Canada, 1996). <http://strategis.ic.gc.ca/SSG/ca00257e.html>.

Lawson, Ian, *Privacy and Free Enterprise: The Legal Protection of Personal Information in the Private Sector* (Ottawa: Public Interest Advocacy Centre, 1992).

Lloyd, Ian, "An Outline of the European Data Protection Directive," (1996) 1 *The Journal of Information, Law and Technology*. <http://elj.warwick.ac.uk/elj/jilt/dp/intros/>.

Louis Harris & Associates and Westin, Dr. Alan F. *The Equifax Canada Report on Consumers and Privacy in the Information Age* (Ville d'Anjou, Quebec: Equifax Canada Inc., 1995).

Maxeiner, J.R. "Business Information and "Personal Data": Some Common-Law Observations About the EU Draft Data Protection Directive," (1995) 80 *Iowa Law Review* 619.

The Office of the Information and Privacy Commissioner of British Columbia, *Visions for Privacy in the 21st Century: A Search for Solutions*. Materials for a conference organized by The Office of the Information and Privacy Commissioner of British Columbia and The University of Victoria. (Victoria, British Columbia: The Office of the Information and Privacy Commissioner of British Columbia, 1996).

Office of the Privacy Commissioner of New Zealand, Fact Sheets on the *Privacy Act 1993* (August 1993). <http://io.knowledge-basket.co.nz/privacy/facts/fact0.htm>.

Office of the Privacy Commissioner of New Zealand, *Review of the Privacy Act 1993: Discussion Papers 1 to 12* (September 1997). <http://www.knowledge-basket.co.nz/privacy/discpp/intro.htm>.

Ontario, Commission on Freedom of Information and Individual Privacy, *Privacy and Personal Data Protection: Research Publication No. 15* (March 1980).

Onyshko, Thomas S. "Access to personal information: British and Canadian Legislative Approaches." (1989) 18 *Manitoba Law Journal* 213.

Onyshko, Thomas S. "The Federal Court and the *Access to Information Act*," (1993) 22 *Manitoba Law Journal* 73.

Onyshko, Thomas S. *Informational Privacy and the Law in Canada* (LL.M. Thesis, University of Toronto, 1995).

Onyshko, Thomas S. "Privacy, Access to Information and Transborder Data Transfer," (Smith Lyons, 1997). <http://www.smithlyons.ca/it/privacy/index.htm>.

Onyshko, Thomas S. and Owens, Richard C. "Debit Cards and Stored Value Cards: Legal Regulation and Privacy Concerns," (1997) 16 *National Banking Law Review* 65.

Owens, Richard C., Onyshko, Thomas S. and Goode, Peter C. "Reform Proposals Relating to Customer Privacy and Tied Selling in the Federally-Regulated Financial Services Sector", in *The Regulation of Financial Institutions: Issues and Perspectives* (Scarborough, Ont.: Carswell, 1997).

Owens, Richard, "Retailing of Financial Services". Paper presented to a Canadian Institute conference (Toronto: The Canadian Institute, 1996).

Owens, Richard, "Some Privacy Thoughts", from *Privacy in Financial Services* (Toronto: The Canadian Institute, 1994).

Owens, Richard, "Steering Clear of the Legal Pitfalls of Database and Relationship Marketing." Paper presented to a Canadian Institute conference (Toronto: The Canadian Institute, 1994).

Owens, Richard, "Some Legal Issues Concerning Databases and Database Marketing", from *Retailing Financial Services* (Toronto: The Canadian Institute, 1995 and 1996).

Owens, Richard and Onyshko, Thomas S., "Legal Regulation and Privacy Concerns Relating to Credit Cards, Debit Cards and Stored Value-Cards", from *Maximizing Your Upside from Credit/Debit/Smart/Cards* (Toronto: The Canadian Institute, 1997).

Owens, Richard and Myers, John, "Privacy in Financial Services: An Overview of Canadian Law", from *Retailing Financial Services* (Toronto: The Canadian Institute, 1994).

Owens, Richard, "Legal Issues in the Creation, Management and Exploitation of Corporate Databases", from *Protecting and Managing IP Assets* (Federated Press, 1997).

Perey A. and Janisch H. "International Restrictions on the Exchange of Information: Privacy, Transborder Data Flows and Trade in Services" from *Privacy in Financial Services: Striking a Balance between Privacy Rights and Profits* (1994: The Canadian Institute).

Privacy & American Business, *Privacy in Cyberspace: Issues and Solutions*. Materials for the Third Annual Conference "Managing Privacy in Cyberspace and Across National Borders" (Hackensack, N.J.: Privacy & American Business, 1996).

Privacy & American Business, *Sourcebook on Business and Global Data Protection*. Materials for the "Third Annual National Conference Managing Privacy in Cyberspace and Across National Borders" (Citicorp Bank, 1996).

Privacy Commissioner of Australia, *Information Privacy in Australia: A National Scheme for Fair Information Practices in the Private Sector* (August 1997). http://www2.austlii.edu.au/itlaw/national_scheme/national-INFORMAT.html.

Prosser, W.L. "Privacy," (1960) 48 *California Law Review* 383.

Public Interest Advocacy Centre/Fédération nationale des associations de consommateurs du Québec, *Surveying Boundaries: Canadians and their Personal Information* (Ottawa and Montreal: PIAC and FNACQ, 1995).

Rankin, M. "Privacy and Technology: A Canadian Perspective," (1984) 22 *Alberta Law Review* 323.

Reidenberg, Joel R. "Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms," (1993) 6 *Harvard Journal of Law & Technology* 287.

Roberts, R.J. "Is Information Property?" (1987) *Intellectual Property Journal* 209.

Rosenbaum, J.I. "The European Commission's Draft Directive on Data Protection," (1992) 33 *Jurimetrics Journal of Law, Science and Technology* 1.

Ryan, E.R. "Privacy, Orthodoxy and Democracy," (1973) 51 *Canadian Bar Review* 84.

Schwartz, P.M. "European Data Protection Law and Restrictions on International Data Flows," (1995) 80 *Iowa Law Review* 471.

Simitis, Spiros, "From the Market to the Polis: The EU Directive on the Protection of Personal Data," (1995) 80 *Iowa Law Review* 445.

Slane, Bruce, *Privacy Law Issues – Reform Proposals and their Impact on the Financial Industry*. Notes for an Address by the Privacy Commissioner for New Zealand, Bruce Slane, to the Fourteenth Annual Banking Law and Practice Conference (May 22, 1997). <http://www.knowledge-basket.co.nz/privacy/speeches/banksyd2.htm>.

Stallworthy, M. "Data Protection: Regulation in a Deregulatory State," (1990) 11 *Statute Law Review* 130.

U.K. Home Office, *Consultation Paper on the EC Data Protection Directive (95/46/EC)* (March 1996). http://www.open.gov.uk/home_off/ccpd/dataprot.htm.

U.K. Home Office, *Consultation Paper on the EC Data Protection Directive (95/46/EC): Response of the Data Protection Registrar* (July 1996) <http://www.open.gov.uk/dpr/answer/content.htm>.

U.K. Home Office, *Data Protection: the Government's Proposals* (July 1997). <http://www.homeoffice.gov.uk/datap2.htm>.

Warren, S.D. and Brandeis, L.D. "The Right to Privacy," (1890) 4 *Harvard Law Review* 193.

Wellbery, B.S. "An Overview of Information Privacy in the United States and European Union," from L. Fischer and R. Bennett, eds., *Privacy in Electronic Commerce: A Compendium of Essays on the Use of Information* (Washington: American Bankers Association, 1997).

Westin, A.F. *Privacy and Freedom* (New York: Atheneum, 1967).

Wiebe, Andreas, "Harmonization of Data Protection Law in Europe," (1996) 3 *The Journal of Information, Law and Technology*. <http://lrc.law.warwick.ac.uk/jilt/confs/3dp/default.htm>.

Wright, Tom, *Privacy Protection Models for the Private Sector* (Toronto: Information and Privacy Commissioner/Ontario: 1996). http://www.ipc.on.ca/web_site.eng/matters/sum_pap/papers/models-e.htm.

